NOTES ON SET THEORY

1. Introduction

Throughout mathematics, sets are used as one of several fundamental types of mathematical objects, along with numbers, ordered pairs, functions, etc. But it turns out that sets are special, in that every other type of mathematical object can be "compiled" into sets. For example:

- A function $f : X \to Y$ can be "compiled" into the set of ordered pairs $\{(x, f(x)) \mid x \in X\}$, sometimes called its **graph**; see Definition 2.42 and Remark 2.47.
- An ordered pair (x, y) can be "compiled" into the set $\{\{x\}, \{x, y\}\}$ (among many other possibilities); see Definition 2.30 and Exercise 2.31.
- The natural number 3 can be "compiled" into $\{0, 1, 2\}$, where $2 := \{0, 1\}$, $1 := \{0\}$, and $0 := \varnothing = \{\}$; thus
$$3 = \{\{\}, \{\{\}\}, \{\{\}, \{\{\}\}\}\}.$$

In this role, set theory serves as the "machine language" (or if you prefer, "assembly language") underlying the higher-level language of ordinary math. Part of the goal of this course is to introduce this "machine language" and the "compilation" process from higher-level math.

Aside from serving as a low-level foundations for the rest of math, set theory also studies several mathematical concepts of fundamental importance in their own right, such as induction, cardinality, and choice. You've surely encountered instances of these concepts already in other areas; in this course, we will define them and develop their basic theory in full generality.

2. Axioms of set theory

Informally, a **set** A is a collection of objects. Given A and some other object x, you are allowed to ask whether or not x is in the collection A, denoted
$$x \in A.$$
Moreover, this is the *only* feature of a set: it is completely determined by what all of its elements are. This is captured by the

Axiom 2.1 (Extensionality)**.** For two sets A, B,
$$A = B \iff \forall x\, (x \in A \iff x \in B).$$

The word "axiom" means that this assertion is *assumed*, rather than *proved* as a theorem would be. Every theorem in math must be proved from simpler assertions; we must necessarily start somewhere, with some basic statements we consider so intuitively unobjectionable that we're willing to take them on faith, hence declare them to be *axioms*.

Similarly, we must take some basic mathematical concepts as undefined in terms of simpler ones. Recall also that in set theory, all other mathematical objects are defined from sets. Thus, formally:

Definition 2.2. The word **set** is a synonym for "mathematical object", and is left undefined.

There is a binary relation $\in$ between sets, also undefined. That is, for any sets (i.e., mathematical objects) x, A, we can connect these two "nouns" via the "verb" $\in$ into the "complete sentence"
$$x \in A.$$
This complete sentence does not "mean" anything; the only thing we know about it is that the Axiom of Extensionality holds (not because of any justification, but only because we said so).

2.A. **Comprehension.** Conceptually, the Axiom of Extensionality tells us that sets turn *assertions*, i.e., "complete sentences", into *objects*, i.e., "nouns". In math, as in English, these are two entirely distinct grammatical categories:

- "It snowed a lot this winter" is a complete sentence.
- "That it snowed a lot this winter" is *not* a complete sentence, but rather a noun (phrase).
- "It is true that it snowed a lot this winter" is again a complete sentence, with the same meaning as the first sentence.
- "It is false that it snowed a lot this winter" is also a complete sentence, with an entirely different meaning.
- "I know that it snowed a lot this winter" is also a complete sentence, with a third meaning.

Similarly:

- $\mathbb{R}$ (the set of real numbers) is a noun.
- "$x \in \mathbb{R}$" is a complete sentence (that depends on the variable x).
- "$x \notin \mathbb{R}$" is a complete sentence with a different meaning.

The Axiom of Extensionality tells us that a set A (noun) is completely determined by the meaning of the assertion "$x \in A$". What about the reverse procedure, the mathematical analog of the English word "that", to turn an assertion (depending on a variable) into a set?

Axiom 2.3 (Comprehension)**.** For any mathematical assertion $\phi(x)$ depending on a variable x, there is a (unique, by Extensionality) set A such that

$$\forall x\,(x \in A \iff \phi(x)).$$

This set A is denoted

$$\{x \mid \phi(x)\}.$$

Here, by a "mathematical assertion", we mean an assertion that can be expressed using the basic binary relation $\in$, as well as the basic equality relation $=$, using the usual logical operations of "and", "or", "not", $\exists$, and $\forall$. The variable x is allowed to appear in this expression, as are any previously known mathematical objects (i.e., sets).[1]

Example 2.4. $\varnothing$ is an abbreviation for $\{x \mid \text{false}\}$, where "false" is a nullary "or", or if you prefer, some arbitrary trivially false statement, such as "$x \neq x$".

Similarly, for finitely many objects $x_1, \ldots, x_n$, let $\{x_1, \ldots, x_n\} := \{x \mid x = x_1 \text{ or } \cdots \text{ or } x = x_n\}$.

Example 2.5. For a set X and assertion $\phi(x)$, define the abbreviation

$$\{x \in X \mid \phi(x)\} := \{x \mid x \in X \ \&\ \phi(x)\}.$$

Example 2.6. For two sets A, B, define the abbreviation

$$A \subseteq B \ :\iff \forall x\,(x \in A \implies x \in B).$$

Then for a set X, its **powerset** is

$$\mathcal{P}(X) := \{A \mid A \subseteq X\} = \{A \mid \forall x\,(x \in A \implies x \in X)\}.$$

[1]Formally, ϕ should be a first-order formula in the signature of set theory $\{\in\}$, with some free variables, and with other sets assigned to all variables except for x. That is, if $y_1, \ldots, y_n$ are the other free variables except x appearing in ϕ, then the "Axiom of Comprehension" is really an axiom schema, consisting of the sentence

$$\forall y_1 \cdots \forall y_n\, \exists A\, \forall x\,(x \in A \iff \phi)$$

for each such formula ϕ.

Example 2.7. If $\mathcal{A}$ is a set of sets (this allows us to avoid having to define what an "indexed collection of sets $(A_i)_{i\in I}$" means, for now; see Definitions 2.59 and 2.60), then define

$$\bigcup \mathcal{A} := \{x \mid \exists A \in \mathcal{A}\,(x \in A)\},$$
$$\bigcap \mathcal{A} := \{x \mid \forall A \in \mathcal{A}\,(x \in A)\},$$

where as usual,

$$\exists A \in \mathcal{A}\,(\cdots) \iff \exists A\,(A \in \mathcal{A}\ \&\ \cdots),$$
$$\forall A \in \mathcal{A}\,(\cdots) \iff \forall A\,(A \in \mathcal{A} \implies \cdots).$$

In particular, if $\mathcal{A} = \{A, B\}$ (per Example 2.4),

$$A \cup B := \bigcup\{A, B\},$$
$$A \cap B := \bigcap\{A, B\}.$$

Definition 2.8. Naive Set Theory consists of the Axioms of Extensionality and Comprehension.

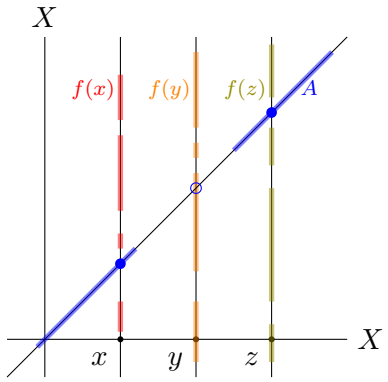
The above examples, along with the brief descriptions from the Introduction of how other standard mathematical notions may be "compiled", should help to convince you that all of "normal" math, i.e., outside of set theory, may be "compiled" into Naive Set Theory. Unfortunately, Naive Set Theory is too powerful for its own good:

2.B. **Cantor's theorem and Russell's paradox.**

Theorem 2.9 (Cantor)**.** Let X be a set, $f : X \to \mathcal{P}(X)$ be a function. Then f is not surjective, i.e., there is an $A \in \mathcal{P}(X)$ such that for all $x \in X$, $f(x) \neq A$.

Of course, we have not yet reduced the notion of "function" to sets – see Definition 2.42. Thus, for now, functions should be understood in the informal sense you're used to from "ordinary" math.

Before giving the one-line proof, we first explain the idea. We want to find a subset $A \subseteq X$ which does not equal any $f(x)$, which by Extensionality means that $A, f(x)$ must differ on the membership of at least one element. Luckily for us, we have just enough elements of X to allocate an element for $A, f(x)$ to differ on for each x: namely, we may allocate x itself. Here is a picture:



We visualize the set X as a (horizontal) line, and each of the subsets $f(x) \subseteq X$ as a subset of the same (vertical) line, so that the entire function f is represented as a subset of the plane X^2. The set A is defined as the subset of the (diagonal) line consisting of precisely the elements not on each vertical line; thus it cannot equal any of the vertical lines. This proof technique is therefore called **diagonalization**.

Proof. Let $A := \{x \in X \mid x \notin f(x)\}$. Then for all $x \in X$, $x \in A \iff x \notin f(x)$, so $A \neq f(x)$. □

Corollary 2.10 (Russell's paradox)**.** Naive Set Theory is inconsistent (self-contradictory).

Proof. Let $V = \{x \mid \text{true}\}$ be the set of all sets (where as in Example 2.4, "true" is a nullary "and", or if you prefer, some trivially true statement such as $x = x$). Note that $V = \mathcal{P}(V)$ (since all objects are sets). Thus $\text{id} : V \to V = \mathcal{P}(V)$ is a surjection, contradicting Cantor's theorem. □

If we "plug in" the above proof of Cantor's theorem into this proof, we get:

Proof. Let $A := \{x \mid x \notin x\}$. Then $A \in A \iff A \notin A$, a contradiction. □

Note that this latter proof shows that Comprehension, rather than Extensionality, is the problem. Namely, Comprehension is too "absolutist": there are general principles of logic[2] which tell us that in any reasonable formalized "mathematical universe", there will always be informal "meta-concepts" that our universe cannot "see". In set theory, this takes the form of "properties" $\phi(x)$: each such property does define an informal "meta-collection" of mathematical objects; but Russell's paradox says that this collection cannot itself always be an object in the mathematical universe.

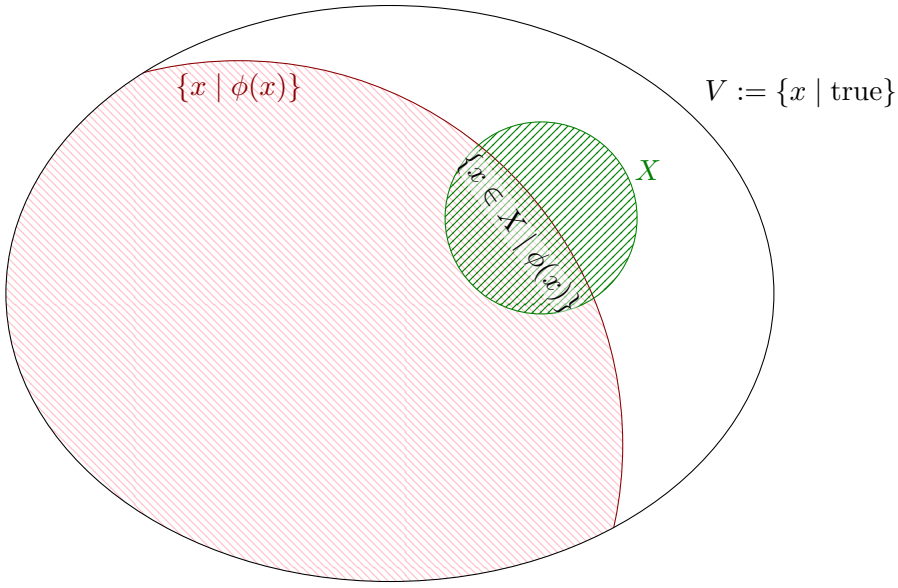
Definition 2.11. A **class** is an informal collection $\{x \mid \phi(x)\}$ defined by a property $\phi(x)$. That is, "class" is roughly synonymous with "property"/"mathematical assertion"/"first-order formula" $\phi(x)$, except that we think of it as the collection defined by $\phi(x)$, rather than the expression $\phi(x)$ itself.[3]

We say that a class $\{x \mid \phi(x)\}$ **is a set** if that instance of Comprehension holds, i.e., there is a (unique, by Extensionality) set A such that $\forall x\,(x \in A \iff \phi(x))$.

A class which is not a set is called a **proper class**. For example, the class in the second proof of Russell's paradox above is a proper class.

2.C. **The theory $\mathsf{ZF}^- - \mathsf{Infinity}$.** The most common way[4] out of Russell's paradox is to restrict the Axiom of Comprehension so that only "sufficiently small" classes form sets.

(2.12)



Intuitively speaking, we allow ourselves to build new sets whose "sizes are bounded" in terms of preexisting ones. For example,

[2] e.g., the Gödel incompleteness theorems, and Tarski's undefinability of truth

[3] Warning: one can easily formalize these "expressions" into mathematical objects, e.g., finite strings of symbols such as $\wedge, \vee, \exists, \in$, etc. But it is then impossible to define, within the language of set theory itself, what such a formalized expression $\phi(x)$ means; this is known as Tarski's undefinability of truth.

[4] Two other approaches, which we will not discuss in detail, are to (a) declare the formula "$x \notin x$" appearing in Russell's paradox to be invalid, because the elements of a set should always be "simpler" than the set itself, leading to a theory called Quine's New Foundations; or (b) disallow the formula "$x \notin x$" because it mentions *negation* without restricting the size of the defined class, leading to a theory called Positive Set Theory.

Axiom 2.13 (Powerset)**.** For any set X, the class $\mathcal{P}(X) = \{A \mid A \subseteq X\}$ from Example 2.6 is a set.

This comprehension is allowed, because even though the size of $\mathcal{P}(X)$ will always be bigger than that of X (formally, by Cantor's theorem; see Theorem 4.35), the size only grows by a "controlled" amount. Similarly,

Axiom 2.14 (Union)**.** For any set $\mathcal{A}$, $\bigcup \mathcal{A} = \{x \mid \exists A \in \mathcal{A}\,(x \in A)\}$ from Example 2.7 is a set.

Axiom 2.15 (Finite Sets)**.** For any $x_1, \ldots, x_n$, $\{x_1, \ldots, x_n\}$ from Example 2.4 is a set.[5]

As is typical throughout math, instead of assuming an n-ary "combining" operation, it is enough to assume the nullary and binary cases:

Axiom 2.16 (Empty Set)**.** $\varnothing = \{x \mid \text{false}\}$ (Example 2.4) is a set.

Axiom 2.17 (Pairing)**.** For any x, y, $\{x, y\} = \{z \mid x = z \text{ or } y = z\}$ is a set.

Proof of Finite Sets from Union, Empty Set and Pairing. By induction on n.[6] For $n = 0$ this is by Empty Set. If $\{x_1, \ldots, x_n\}$ is a set, then $\{x_1, \ldots, x_n, x_{n+1}\} = \bigcup\{\{x_1, \ldots, x_n\}, \{x_{n+1}, x_{n+1}\}\}$. □

The preceding axioms all allow us to build new sets that are slightly bigger than existing ones. We now introduce two axiom schemas that say directly that a class smaller than a set is a set.

Axiom 2.18 (Restricted Comprehension/Separation)**.** Any class contained in a set is a set.

That is, for any property $\phi(x)$ (as in the original Comprehension 2.3) and set X, if $\{x \mid \phi(x)\} \subseteq X$, meaning $\forall x\,(\phi(x) \implies x \in X)$, then $\{x \mid \phi(x)\}$ is a set.

Equivalently, for any $\phi(x)$ and set X, the intersection $X \cap \{x \mid \phi(x)\} = \{x \in X \mid \phi(x)\}$ from Example 2.5 is a set; this is depicted in the above picture (2.12).

Proof that these two axioms are equivalent. Assuming that any class contained in X is a set, then

$$\{x \in X \mid \phi(x)\} = \{x \mid x \in X \ \&\ \phi(x)\}$$

is a class contained in X, hence is a set.

Conversely, assuming $\{x \in X \mid \phi(x)\}$ is always a set, we have

$$\begin{aligned} \{x \mid \phi(x)\} \subseteq X &\iff \forall x\,(\phi(x) \implies x \in X) && \text{by definition of } \subseteq \\ &\iff \forall x\,(\phi(x) \iff x \in X \ \&\ \phi(x)) \\ &\iff \{x \mid \phi(x)\} = \{x \in X \mid \phi(x)\} && \text{which is a set.} \end{aligned}$$

□

Example 2.19. $V = \{x \mid \text{true}\}$ is not a set. If it were, then every Comprehension $\{x \mid \phi(x)\}$ would reduce to the Restricted Comprehension $\{x \in V \mid \phi(x)\}$, recovering in particular Russell's paradox.

Example 2.20. For any nonempty set $\mathcal{A}$, $\bigcap \mathcal{A} = \{x \mid \forall A \in \mathcal{A}\,(x \in A)\}$ from Example 2.7 is a set.

Proof. Fix $A_0 \in \mathcal{A}$. Then

$$\bigcap \mathcal{A} = \{x \in A_0 \mid \forall A \in \mathcal{A}\,(x \in A)\},$$

since for any x,

$$\forall A \in \mathcal{A}\,(x \in A) \iff x \in A_0 \ \&\ \forall A \in \mathcal{A}\,(x \in A).$$

□

Remark 2.21. For $\mathcal{A} = \varnothing$, the same definition of $\bigcap \mathcal{A}$ would yield the entire universe V.

In mathematical practice, one typically only intersects subsets $A \subseteq X$ of a fixed, context-dependent ambient set X (e.g., closed subsets of a topological space, subgroups of a group, ...). In such contexts, the "right" convention is to define the nullary intersection $\bigcap \varnothing := X$.

[5] This would be an axiom schema.

[6] Formally, this induction is taking place in the metatheory, i.e., this is really a *proof schema*: for each n, we get a different proof of the corresponding axiom in the axiom schema of Finite Sets.

While Restricted Comprehension says that any subclass of a set is a set, one might expect more generally that a class which "injects" into a set ought also be a set. Relatedly, one might also expect that a class which admits a "surjection" from a set ought also be a set. One needs to be careful about what this "injection"/"surjection" means: if we assume it is given by a function which is already a set, then that more-or-less defeats the purpose, since this function will already be an "upper bound" on its domain/range (see Exercise 2.40). Hence, we need to work once again with "meta-collections", i.e., properties, this time of pairs:

Axiom 2.22 (Replacement)**.** Let $\phi(x, y)$ be a property of *two* variables x, y (and possibly depending on other known objects). For any set X, if

$$\forall x \in X \underbrace{\forall y \forall z \, (\phi(x, y) \ \& \ \phi(x, z) \implies y = z)}_{\text{"}\exists \text{ at most one } y \text{ s.t. } \phi(x,y)\text{"}},$$

then $\{y \mid \exists x \in X \, \phi(x, y)\}$ is a set.

This axiom is quite powerful:

Exercise 2.23. Prove Restricted Comprehension from Replacement and no other axioms (except Extensionality).

Exercise 2.24. Another common version of Replacement uses "$\exists!$" instead of "$\exists$ at most one".

(a) Prove Restricted Comprehension from this version of Replacement and Empty Set.
(b) Prove that the two versions of Replacement are equivalent, using only Empty Set.
(c) Prove yet another version of Replacement that uses "$\exists$ at most a set of":

$$\forall x \in X \, \exists A \, \forall y \, (\phi(x, y) \implies y \in A).$$

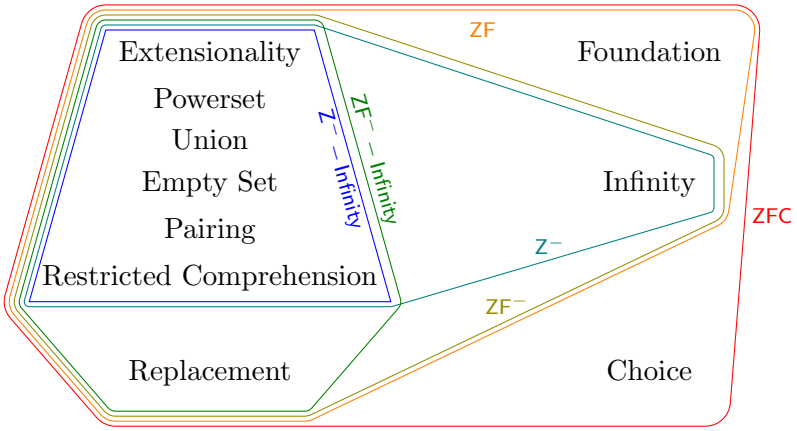
(You may use Extensionality and all axioms from this subsection.)

Exercise 2.25. Prove Pairing from Replacement, Empty Set, and Powerset.

Definition 2.26. The set theory $\mathsf{ZF}^- - \mathsf{Infinity}$ consists of the Axioms of Extensionality (2.1), Powerset (2.13), Union (2.14), Empty Set (2.16), Pairing (2.17), and Replacement (2.22); we thus also have Restricted Comprehension (2.18) by Exercise 2.23.

The awkward name with two minus signs is because this theory is lacking two important axioms, Foundation and Infinity, from the theory known as ZF that will be introduced later; see Axioms 3.100 and 3.152. Adding the further Axiom of Choice 3.203 yields the set theory known as ZFC, which is widely accepted as the "standard" foundations for mathematics.

(2.27)



2.D. **Ordered pairs, Cartesian products, relations, functions.** We now begin to discuss the process of "compiling" other types of commonly used mathematical objects into sets. Broadly speaking, this goes as follows. For the given type of object, we formulate some axioms for it as if it were primitive, that capture everything we need to know when using this type of object in mathematical practice. We then "encode" this type of object into sets, and then prove the desired axioms from the set theory axioms. There may be many reasonable such "encodings", in which case it doesn't matter which one we pick: once we've proved the axioms, we know all we need to use the definition in practice, and never need to think about the encoding again.[7]

For ordered pairs, we need to know two things about them in practice:

(2.28) For any mathematical objects x, y, there is another object called the pair (x, y).

(2.29) ("Extensionality for pairs") The *only* feature of an ordered pair is its two coordinates:

$$(a, b) = (c, d) \iff a = c \ \& \ b = d.$$

Definition 2.30 (Kuratowski)**.** For any x, y, let $(x, y) := \{\{x\}, \{x, y\}\}$.

Proof of (2.28). This is indeed a set, by the Axiom of Pairing (2.17) applied thrice. □

Proof of (2.29). $\Longleftarrow$ is obvious (note: unlike in Extensionality for sets (2.1), where $\Longrightarrow$ was the obvious direction[8]). Now suppose $(a, b) = (c, d)$. Then $\{a\} \in (a, b) = (c, d) = \{\{c\}, \{c, d\}\}$, whence $\{a\} = \{c\}$ or $\{c, d\}$, both of which contain c, whence $c \in \{a\}$, whence $c = a$. So

$$\{\{a\}, \{a, b\}\} = (a, b) = (c, d) = (a, d) = \{\{a\}, \{a, d\}\}.$$

If $a = b$, then the LHS is $\{\{a\}\}$, hence so is the RHS, hence $\{a, d\} = \{a\}$, hence $d = a = b$. Otherwise, $\{a, b\}$ in the LHS must equal $\{a, d\}$ in the RHS (since it is not $\{a\}$ which does not contain b), hence $b \in \{a, b\} = \{a, d\}$, hence $b = d$ (since $b \neq a$). □

Exercise 2.31. Which of the following encodings also work, i.e., also satisfy (2.28) and (2.29)?

(a) $(x, y) := \{x, y\}$
(b) $(x, y) := \{x, \{y\}\}$
(c) $(x, y) := \{\{0, x\}, \{1, y\}\}$
(d) $(x, y) := \{x, \mathcal{P}(y)\}$
(e) $(x, y) := \{\mathcal{P}(x), \mathcal{P}(y) \setminus \{\varnothing\}\}$
(f) $(x, y) := \{x, \{x, y\}\}$ [Hint: this depends on whether the Axiom of Foundation (3.100) holds.]

Definition 2.32. For two classes X, Y, their **Cartesian product** is

$$X \times Y := \{(x, y) \mid x \in X \ \& \ y \in Y\} = \{p \mid \exists x \in X \, \exists y \in Y \, (p = (x, y))\}.$$

Proposition 2.33. If X, Y are sets, then so is $X \times Y$.

Proof. For each x, for each y, we have a set (x, y); thus by Replacement (applied to $\phi(y, p) :\Longleftrightarrow p = (x, y)$), we have a set $\{x\} \times Y = \{p \mid \exists y \in Y \, (p = (x, y))\}$; thus by Replacement again (applied to $\psi(x, s) :\Longleftrightarrow s = \{p \mid \exists y \in Y \, (p = (x, y))\}$), we have a set

$$\{\{p \mid \exists y \in Y \, (p = (x, y))\} \mid x \in X\};$$

now take Union. □

[7] Again, a computer analogy is helpful: the only type of data on (modern) computers is bytes, i.e., strings of 8 bits. On my computer, the letter 'M' is encoded as the byte 01001101_2, while on yours it may be 11010100_2; in programming practice (that's not super-low-level, e.g., hardware drivers), we never need to think about these encodings.

[8] There is a philosophical distinction between the notions of sets vs. pairs (other than that only the former can serve as a foundation for mathematics). Pairs are known as a *positive type* of object, in that they are originally specified by how they are *created*: by combining two other objects (2.28). Thus, the nontrivial direction of Extensionality for pairs says that if two pairs are the same, then they must have been created the same way. By contrast, sets (in the set-theoretic sense) are a *negative type* of object, being specified by how they may be *used*: by asking if some x is $\in$ it. The nontrivial direction of Extensionality says that if two sets look the same when used, then they are the same.

Exercise 2.34. Give a different proof that $X \times Y$ is a set, using Powerset instead of Replacement, that however has the disadvantage of depending on our specific chosen encoding of pairs.

Definition 2.35. As indicated above, if $F(x)$ is a mathematical *expression* (rather than assertion) that depends on a variable x, and X is a set, we use the shorthand

$$\{F(x) \mid x \in X\} := \{y \mid \exists x \in X\, (F(x) = y)\},$$

which is a set by Replacement. Here, by "mathematical expression", we really mean a "meta-function", i.e., its graph is a "meta-relation" defined by a property $\phi(x, y)$ as in the statement of Replacement (2.22).

Definition 2.36. A set (or class) R is a **binary relation** if each of its elements is an ordered pair (x, y), in which case we write

$$x\ R\ y \ :\iff\ (x, y) \in R.$$

Conversely, if $\bowtie$ is a symbol that already denotes some binary relation, then we abuse notation by also using $\bowtie$ to denote the class defined by the above. For example,

$$\in\ = \{(x, y) \mid x \in y\}.$$

Exercise 2.37. Show that this is a proper class.

Definition 2.38. The **domain** and **range** of a binary relation R are

$$\mathrm{dom}(R) := \{x \mid \exists y\, ((x, y) \in R)\},$$
$$\mathrm{rng}(R) := \{y \mid \exists x\, ((x, y) \in R)\}.$$

Proposition 2.39. If R is a set, then so are $\mathrm{dom}(R), \mathrm{rng}(R)$.

Proof. By Replacement: $\mathrm{dom}(R) = \{x \mid \exists p \in R\, \exists y\, (p = (x, y))\}$, and for each p, there is at most one x such that $\exists y\, (p = (x, y))$, by "Extensionality for pairs" (2.29); similarly for $\mathrm{rng}(R)$. □

Exercise 2.40. Give another proof using Union instead of Replacement, assuming the Kuratowski encoding of pairs (cf. Exercise 2.34).

Corollary 2.41. If R is a binary relation and also a set, then it is a subset of $X \times Y$ for some sets X, Y. In that case, we call R a **binary relation between** X, Y.

Proof. $X := \mathrm{dom}(R)$, $Y := \mathrm{rng}(R)$ works. □

Definition 2.42. A relation f is a **function** if for each x, there is at most one y such that $x\ f\ y$. If such unique y exists, then we denote it by $f(x)$.

If f is a function, $\mathrm{dom}(f) = X$, and $\mathrm{rng}(f) \subseteq Y$, then we say that f is a **function from** X **to** Y, denoted $f : X \to Y$, and call Y a **codomain** of f.

Outside of set theory, functions are usually treated as a primitive type of object, distinct from sets, much as pairs are. The following axioms dictate how we use functions in practice:[9]

(2.43) If $f : X \to Y$ is a function, and $x \in X$, then we get an object $f(x) \in Y$.

(2.44) ("Extensionality for functions") For two functions $f, g : X \to Y$, we have

$$f = g \iff \forall x \in X\, (f(x) = g(x)).$$

(2.45) ("Comprehension for functions") To define a function $f : X \to Y$, specify for each $x \in X$ a unique $f(x) \in Y$. That is, specify a property $\phi(x, y)$ such that $\forall x \in X\, \exists! y \in Y\, \phi(x, y)$.

Exercise 2.46. Verify that the encoding of functions as sets of pairs satisfies these axioms.

[9] The form of these axioms shows that functions are a *negative type*, like sets; cf. Footnote 8.

Remark 2.47. Unlike with pairs (see Exercise 2.31), this standard encoding of functions subjectively feels fairly "canonical", and does not involve the same level of trickery as the encoding of pairs.

Nonetheless, we should still keep in mind the distinction between the *concept* of a function, which is still best thought of as primitive, and its *encoding* as a set of pairs. To emphasize this distinction, people usually define the **graph** of a function $f : X \to Y$ to mean

$$\{(x, f(x)) \mid x \in X\},$$

which formally is the same as f under the standard encoding, but explicitly indicates that we are thinking of f as a set of pairs rather than a function.

Definition 2.48. For two classes X, Y,

$$Y^X := \{f \mid f \text{ is a function } X \to Y\}.$$

This is an abuse of notation: there are several other operations denoted the same way in set theory (see Remark 2.67, Exercise 3.172, Remark 4.32). Less ambiguous notations people sometimes use include ${}^X Y, \mathrm{Fun}(X, Y)$. We think these are too ugly and/or verbose, and so will depend on context for clarity.

Corollary 2.49 (of Definition 2.32)**.** For sets X, Y, so is Y^X.

Proof. Y^X is a set of sets of pairs, i.e., $Y^X \subseteq \mathcal{P}(X \times Y)$. □

We assume you are familiar with other standard concepts related to functions, and will have no difficulties formalizing them into set theory:

Definition 2.50. For relations $R \subseteq X \times Y$ and $S \subseteq Y \times Z$, their **composition** is

$$S \circ R := \{(x, z) \in X \times Z \mid \exists y \in Y\, (x\ R\ y\ S\ z)\}$$
$$(\text{shorthand for } \{p \in X \times Z \mid \exists x \in X\, \exists y \in Y\, \exists z \in Z\, (p = (x, z)\ \&\ x\ R\ y\ \&\ y\ S\ z)\}).$$

(As usual, the order is "wrong", ultimately so that we can write $f(x)$ rather than $(x)f$.)

Exercise 2.51. Prove that if $f : X \to Y$ and $g : Y \to Z$ are functions, then so is $g \circ f : X \to Z$.

Definition 2.52. The **identity function** is (as a class of pairs) the same as the equality relation $=$. The **identity function on** X is its restriction to X, i.e., intersection with $X \times X$.

Exercise 2.53. Prove that relation composition is associative and has id as identity element.

Example 2.54. The **inverse** of a binary relation R is

$$R^{-1} := \{(y, x) \mid (x, y) \in R\}.$$

Exercise 2.55. Let $R \subseteq X \times Y$ be a binary relation.

(a) What does $R^{-1} \circ R \subseteq \mathrm{id}_X$ mean?
(b) What does $R^{-1} \circ R \supseteq \mathrm{id}_X$ mean?
(c) Prove that R is a function $X \to Y$ iff $R^{-1} \circ R$?? id_X and $R \circ R^{-1}$?? id_Y, where each ?? is either $\subseteq$ or $\supseteq$ (which?).
(d) Conclude that for a function $f : X \to Y$, $f^{-1} : Y \to X$ is also a function iff $\forall y \in Y\, \exists! x \in X\, (f(x) = y)$, i.e., f is a **bijection**.
(e) Show that a function $f : X \to Y$ is **injective**, resp., **surjective** (defined the usual way), iff one of the other inclusions in (c) above holds (which?).

Exercise 2.56. For a relation $R \subseteq X \times Y$, define the **image** $R[A] \subseteq Y$ of a subset $A \subseteq X$, specializing to the case when R is a function; $R^{-1}[B] \subseteq X$ is then the **preimage** of $B \subseteq Y$.

Show that taking image under a relation preserves arbitrary unions (first write what this means), and preserves arbitrary intersections iff $R = f^{-1}$ for a function $f : Y \to X$.

2.E. **Independence of encoding, indexed products and (disjoint) unions.** Bijections provide one way of formalizing the idea that the choice of encoding of ordered pairs, functions, etc., is irrelevant:

Proposition 2.57. Let $(,)$ and $(,)'$ be two ways of encoding ordered pairs, both obeying the axioms (2.28) and (2.29). Then there is a bijection F (between the classes of ordered pairs encoded either way) converting between these encodings, namely

$$F(x,y) := (x,y)'.$$

In particular, for any sets (or classes) X, Y, letting $\times, \times'$ denote the Cartesian products defined using either encoding, the above bijection between *all* pairs restricts to a bijection

$$\begin{aligned} F : X \times Y &\longrightarrow X \times' Y \\ (x,y) &\longmapsto (x,y)'. \end{aligned}$$

Proof. We may certainly define the relation F by the above formula, i.e.,

$$F := \{(p,p') \mid \exists x,y\,(p = (x,y) \ \&\ p' = (x,y)')\}.$$

To check that F is a function, we need to know

$$(p,p'_1),(p,p'_2) \in F \implies p'_1 = p'_2.$$

From $(p,p'_1) \in F$, we get that $p = (x_1,y_1)$ and $p'_1 = (x_1,y_1)'$ for some x_1, y_1, while from $(p,p'_2) \in F$, we get that $p = (x_2,y_2)$ and $p'_2 = (x_2,y_2)'$ for some (*a priori* different) x_2, y_2; but by the extensionality axiom (2.29) for $(,)$, from $(x_1,y_1) = p = (x_2,y_2)$ we get $x_1 = x_2$ and $y_1 = y_2$, whence $p'_1 = (x_1,y_1) = (x_2,y_2) = p'_2$. Similarly, F^{-1} is a function. □

Exercise 2.58. Similarly, for any two ways of encoding functions obeying (2.43) to (2.45), show that we have a bijection $Y^X \cong Y^{X\prime}$ between the respective sets of functions, for any two sets X, Y.

Even if we accept the standard (Kuratowski) encoding of pairs, note that there are two obvious ways to build triples (and higher n-tuples) from pairs:

$$\begin{aligned} (x,y,z)_1 &:= ((x,y),z), \\ (x,y,z)_2 &:= (x,(y,z)). \end{aligned}$$

More generally, in areas such as real analysis we would want to consider "∞-tuples", i.e., infinite sequences $(x_0, x_1, \dots)$; in fact, we may as well consider arbitrary indexed families $(x_i)_{i\in I}$.

Definition 2.59. An **indexed family** $(x_i)_{i\in I}$ over a set or class I is another name for a function f with domain I, where x_i is another name for $f(i)$.

Definition 2.60. For an indexed family of sets $(A_i)_{i\in I}$, define the **indexed union**

$$\textstyle\bigcup_{i\in I} A_i := \bigcup\{A_i \mid i \in I\}$$

(constructed via the Axioms of Union and Replacement).

Exercise 2.61. Show that the concepts of indexed union and union of a set of sets are interchangeable: conversely, for a set of sets $\mathcal{A}$,

$$\textstyle\bigcup \mathcal{A} = \bigcup_{A\in\mathcal{A}} A.$$

Definition 2.62. For an indexed family of sets $(X_i)_{i\in I}$, its **indexed Cartesian product** $\prod_{i\in I} X_i$ is the set of all indexed families $(x_i)_{i\in I}$ where each $x_i \in X_i$.

Proposition 2.63. If $(X_i)_{i\in I}$ is a family of sets indexed over a set I, then $\prod_{i\in I} X_i$ is a set.

Proof. $\prod_{i\in I} X_i \subseteq (\bigcup_{i\in I} X_i)^I$. □

We now have several ways of encoding n-tuples:

Definition 2.64 (preliminary; see Axiom 3.152)**.**

$$\begin{aligned} 0 &:= \varnothing, \\ 1 &:= \{0\}, \\ 2 &:= \{0, 1\}, \\ 3 &:= \{0, 1, 2\}, \\ &\vdots \end{aligned}$$

Exercise 2.65. Let $n \geq 2$. We may encode n-tuples as

$$(x_0, \ldots, x_{n-1}) := (((x_0, x_1), x_2), \ldots x_{n-1})$$

(or any other way of writing the parentheses). We may also regard the tuple as an indexed family over the domain n. Show that there is a canonical bijection converting between these encodings. For example, for $n = 3$, for any sets X_0, X_1, X_2, we have bijections

$$(X_0 \times X_1) \times X_2 \cong \textstyle\prod_{i \in 3} X_i \cong X_0 \times (X_1 \times X_2).$$

Remark 2.66. Of course, we could not have originally defined ordered pairs via indexed families, since functions were defined in terms of ordered pairs. But the above encoding still works for $n = 2$, *given* the concept of function, yielding *another* encoding of ordered pairs.

Remark 2.67. When $(X)_{i \in I}$ is a constant family of sets, note that our definition of $\prod_{i \in I} X$ agrees with the set of functions X^I (Definition 2.48). In particular, X^n is the set of functions $n \to X$, which is in canonical bijection with (not equal to) $((X \times X) \times \cdots) \times X$.

For "canonical" bijections such as those above, it is common in informal mathematical practice to treat them as equalities, by "identifying" elements in both sets. An important feature of *actual* equality is (one direction of) Extensionality: equal things should be interchangeable in all contexts. Of course, the Axiom of Extensionality tells us that this literally holds only for actually equal sets. But for many constructions used in practice, sets in bijection are also "interchangeable":

Definition 2.68. An operation on sets $F(X_0, \ldots, X_{n-1})$, e.g., $\times, \mathcal{P}, \cap$, is called **functorial** (on bijections[10]) if it comes equipped with, for each bijections $f_i : X_i \cong Y_i$, an *induced bijection* $F(f_0, \ldots, f_{n-1}) : F(X_0, \ldots, X_{n-1}) \cong F(Y_0, \ldots, Y_{n-1})$. These induced bijections should respect composition in the f_i: if we have another family of bijections $g_i : Y_i \cong Z_i$, then we require

$$F(g_0, \ldots, g_{n-1}) \circ F(f_0, \ldots, f_{n-1}) = F(g_0 \circ f_0, \ldots, g_{n-1} \circ f_{n-1}).$$

Exercise 2.69. Show that this implies $F(\mathrm{id}_{X_0}, \ldots, \mathrm{id}_{X_{n-1}}) = \mathrm{id}_{F(X_0, \ldots, X_{n-1})}$ and $F(f_0^{-1}, \ldots, f_{n-1}^{-1}) = F(f_0, \ldots, f_{n-1})^{-1}$.

Example 2.70. $\times$ is a functorial binary operation: for $f_0 : X_0 \cong Y_0$ and $f_1 : X_1 \cong Y_1$, we have

$$\begin{aligned} X_0 \times X_1 &\cong Y_0 \times Y_1 \\ (x_0, x_1) &\mapsto (f_0(x_0), f_1(x_1)), \end{aligned}$$

and it is easily seen that this preserves composition in the f_i.

Example 2.71. "Exponentiation", i.e., sets of functions, is functorial: for f_0, f_1 as above, we have

$$\begin{aligned} X_1^{X_0} &\cong Y_1^{Y_0} \\ h &\mapsto f_1 \circ h \circ f_0^{-1} : Y_0 \to X_0 \to X_1 \to Y_1. \end{aligned}$$

[10]The general context for this concept is the area of math called *category theory*, which we will not go into.

Exercise 2.72. Verify that this preserves composition in the f_i.

Exercise 2.73. Show that $\mathcal{P}$ (powerset) is a functorial unary operation on sets.

Example 2.74. $\bigcup$ (union) is *not* a functorial unary operation. For example, $\{\varnothing\} \cong \{\{\varnothing\}\}$, but $\bigcup\{\varnothing\} = \varnothing \ncong \{\varnothing\} = \bigcup\{\{\varnothing\}\}$.

Exercise 2.75. Show that $\cup$ is not a functorial binary operation either.

This reflects the fact that in mathematical practice, it is unusual to take the union of two (or more) sets without knowing something about how they are related. Usually, we only take union of subsets *of a given ambient set*; or else, we take a *disjoint union* of unrelated sets. This latter concept is again defined up to a choice of encoding:

Definition 2.76. For a family of sets $(X_i)_{i\in I}$ indexed over a set I, its **disjoint union** $\bigsqcup_{i\in I} X_i$ is a set equipped with an indexed family of injections $\iota_i : X_i \to \bigsqcup_{j\in I} X_j$ whose images are disjoint and cover $\bigsqcup_{j\in I} X_j$. In other words:

(2.77) For each $i \in I$ and $x \in X_i$, we have a corresponding element $\iota_i(x) \in \bigsqcup_{i\in I} X_i$.

(2.78) Each $y \in \bigsqcup_{i\in I} X_i$ is equal to such an $\iota_i(x)$ for a unique i and $x \in X_i$.

One ("standard") encoding is given by

$$\bigsqcup_{i\in I} X_i := \{(i, x) \in I \times \bigcup_{i\in I} X_i \mid x \in X_i\},$$
$$\iota_i(x) := (i, x).$$

Exercise 2.79. Show that all encodings of disjoint union obeying these axioms are in canonical bijection with each other. Moreover, $\bigsqcup_{i\in I}$ is a functorial "I-ary operation" (define what this means).

We also mention various other "canonical" bijections commonly used throughout math. These are perhaps not all thought of as converting between different "encodings" of the same concept; nonetheless, one frequently abuses notation/terminology by treating them as equalities.

Example 2.80. For any set X, there is a bijection between subsets of X and their **indicator** (or **characteristic**) functions:

$$\mathcal{P}(X) \cong 2^X$$
$$A \mapsto \begin{pmatrix} \chi_A : X \to 2 = \{0,1\} \\ x \mapsto \begin{cases} 1 & \text{if } x \in A, \\ 0 & \text{else} \end{cases} \end{pmatrix}$$
$$f^{-1}[\{1\}] \hookleftarrow f.$$

Example 2.81. For any sets X, Y, Z, we have bijections

$$Z^{X\times Y} \cong (Z^X)^Y$$
$$f \mapsto (y \mapsto (x \mapsto f(x, y)))$$
$$(g(y)(x) \hookleftarrow (x, y)) \hookleftarrow g,$$

and similarly $Z^{X\times Y} \cong (Z^Y)^X$.

Exercise 2.82. Give a bijection $\mathcal{P}(X \times Y) \cong \mathcal{P}(X)^Y$.

Exercise 2.83. For an indexed family of sets $(X_i)_{i\in I}$ and a set Y, give a bijection

$$Y^{\bigsqcup_{i\in I} X_i} \cong \prod_{i\in I} Y^{X_i}.$$

Exercise 2.84. In particular, $\mathcal{P}(\bigsqcup_{i\in I} X_i) \cong \prod_{i\in I} \mathcal{P}(X_i)$.

3. Induction

Now that we have introduced the basics of set theory, we turn to developing the general theory of induction, which will include usual induction for $\mathbb{N}$ as a (very) special case. The general idea is: we have a set X of elements that we're inducting on, and a way of "deriving" new elements from previous ones; we say a *principle of induction* holds if everything can eventually be derived.

3.A. Monotone set operators and the Knaster–Tarski fixed point theorem.

Definition 3.1. A **monotone set operator** $T : \mathcal{P}(X) \to \mathcal{P}(X)$ on a set X is a function obeying

$$\forall A, B \in \mathcal{P}(X)\,(A \subseteq B \implies T(A) \subseteq T(B)).$$

A subset $A \subseteq X$ is **T-closed** if $T(A) \subseteq A$.

There are many possible interpretations of this simple definition. For the purposes of induction, we think of T as specifying, for each subset $A \subseteq X$, the set of new elements $T(A)$ which can be "derived" from A. Being T-closed means that all elements "derivable" from A are already in A.

Example 3.2. We have a monotone set operator on $X = \mathbb{N}$ given by

$$T(A) := \{0\} \cup \{n + 1 \mid n \in A\}.$$

In other words, we start with 0 (the base case), and can derive $n + 1$ from n (the inductive case). The only T-closed subset of $\mathbb{N}$ is all of $\mathbb{N}$ (this will be taken as the *definition* of $\mathbb{N}$; see Axiom 3.152).

Example 3.3. We have another monotone set operator on $\mathbb{N}$, given by

$$\begin{aligned} T(A) &:= \{n \in \mathbb{N} \mid \forall m < n\,(m \in A)\} \\ &= \{n \in \mathbb{N} \mid n \subseteq A\} \quad \text{(recalling Definition 2.64; see also Axiom 3.152).} \end{aligned}$$

This says that n can be derived once we know everything smaller, and corresponds to the principle of "strong induction"; see Example 3.12.

Example 3.4. Let X be any set, and let $(f_i : X^{N_i} \to X)_{i \in I}$ be a family of "N_i-ary operations" on X, where the N_i are arbitrary sets. The set X equipped with such a family $(f_i)_{i \in I}$ is sometimes called an **algebra**, or more verbosely, a *first-order structure over a functional signature*. Examples:

(a) $\mathbb{R}$ equipped with $+ : \mathbb{R}^2 \to \mathbb{R}$, $\cdot : \mathbb{R}^2 \to \mathbb{R}$, $- : \mathbb{R} \to \mathbb{R}$, $0 : \mathbb{R}^0 \to \mathbb{R}$, and $1 : \mathbb{R}^0 \to \mathbb{R}$, or a subset thereof, e.g., only $+, -, 0$.
(b) $\mathbb{R}^n$ equipped with $+ : (\mathbb{R}^n)^2 \to \mathbb{R}^n$ (vector addition), $\vec{0} : (\mathbb{R}^n)^0 \to \mathbb{R}^n$ (zero vector), and for each $a \in \mathbb{R}$, the unary operation $a \cdot (-) : \mathbb{R}^n \to \mathbb{R}^n$ (scalar multiplication).
(c) $\mathcal{P}(X)$ for an arbitrary set X, equipped with $\cap, \cup, \neg, \varnothing, X$ (where $\neg A := X \setminus A$).
(d) $\mathcal{P}(X)$ for an arbitrary set X, equipped with $\bigcap, \bigcup, \neg, \varnothing, X$, where $\bigcap, \bigcup : A^{\mathbb{N}} \to A$.
(e) $\mathbb{N}$ equipped with $0 : \mathbb{N}^0 \to \mathbb{N}$ and $S : \mathbb{N} \to \mathbb{N}$ where $S(n) := n + 1$ (successor).
(f) $\mathbb{N}$ equipped with only $S : \mathbb{N} \to \mathbb{N}$.

We may then define the monotone set operator

$$T(A) := \{f_i(\vec{x}) \mid i \in I \ \&\ \vec{x} \in A^{N_i}\}.$$

A T-closed set is then a set closed under the operations. For example, in (b), a T-closed set is a vector subspace of $\mathbb{R}^n$. In (e), T recovers that from Example 3.2.

Example 3.5. Let X be an arbitrary set, and define the set operator T on X^2 by

$$\begin{aligned} T(A) &:= \{(x, x) \mid x \in X\} \cup \\ &= \{(y, x) \mid (x, y) \in A\} \cup \\ &= \{(x, z) \mid (x, y), (y, z) \in A\}. \end{aligned}$$

Then $A \subseteq X^2$ is T-closed iff A is an equivalence relation on X.

Theorem 3.6 (Knaster–Tarski fixed point)**.** Let $T : \mathcal{P}(X) \to \mathcal{P}(X)$ be a monotone set operator. For every $A \subseteq X$, there is a smallest T-closed $\overline{T}(A) \supseteq A$, called the **$T$-closure** of A, or sometimes the T-closed subset **generated by** A. Moreover, $T(\overline{T}(\varnothing)) = \overline{T}(\varnothing)$.

Proof. The first claim follows from combining the following two useful facts:

Lemma 3.7. For any monotone set operator $T : \mathcal{P}(X) \to \mathcal{P}(X)$, the T-closed sets are closed under arbitrary intersections, i.e., if $\mathcal{A} \subseteq \mathcal{P}(X)$ is a set of T-closed sets, then so is $\bigcap \mathcal{A}$.

(This includes the case $\bigcap \mathcal{A} = \varnothing$ from Remark 2.21.)

Proof. For each $A \in \mathcal{A}$, we have $T(\bigcap \mathcal{A}) \subseteq T(A) \subseteq A$ by monotonicity, whence $T(\bigcap \mathcal{A}) \subseteq \bigcap \mathcal{A}$. □

Proposition 3.8. For any set X and family of subsets $\mathcal{A} \subseteq \mathcal{P}(X)$, the following are equivalent:

(i) $\mathcal{A}$ is closed under intersections (including $\bigcap \varnothing = X$ from Remark 2.21).
(ii) For every $A \subseteq \mathcal{P}(X)$, there is a smallest $\overline{A} \in \mathcal{A}$ such that $A \subseteq \overline{A}$.

(Such an $\mathcal{A} \subseteq \mathcal{P}(X)$ is sometimes called a **closure system**.)

Proof. (i) $\implies$ (ii) Let $\overline{A} := \bigcap\{B \in \mathcal{A} \mid A \subseteq B\}$. Then $\overline{A} \in \mathcal{A}$ since $\mathcal{A}$ is closed under intersections, and every other $B \in \mathcal{A}$ such that $A \subseteq B$ is one of the sets we're intersecting, hence contains $\overline{A}$.
(ii) $\implies$ (i) This follows from the preceding lemma, since $A \mapsto \overline{A}$ is easily monotone: if $A \subseteq B$, then $A \subseteq B \subseteq \overline{B} \in \mathcal{A}$, whence $\overline{A} \subseteq \overline{B}$. □

Finally, to show $T(\overline{T}(\varnothing)) = \overline{T}(\varnothing)$: $\subseteq$ is because $\overline{T}(\varnothing)$ is T-closed; then by monotonicity, $T(T(\overline{T}(\varnothing))) \subseteq T(\overline{T}(\varnothing))$, whence $T(\overline{T}(\varnothing))$ is T-closed, and contains $\varnothing$, whence $\overline{T}(\varnothing) \subseteq T(\overline{T}(\varnothing))$. □

The following is merely a restatement of the definition of $\overline{T}(A)$:

Principle of T-induction for $\overline{T}$. Let $T : \mathcal{P}(X) \to \mathcal{P}(X)$ be a monotone set operator and $A \subseteq X$.

(a) For any $B \subseteq X$, if $A \subseteq B$ and $T(B) \subseteq B$, then $\overline{T}(A) \subseteq B$.
(b) Equivalently, for any property $\phi(x)$, if
- $\forall x \in A$, $\phi(x)$ (base case) and
- $\forall x \in T(\{y \in X \mid \phi(y)\})$, $\phi(x)$ (inductive case),

then $\forall x \in \overline{T}(A)$, $\phi(x)$.

To go between (a) and (b), simply take $B := \{x \in X \mid \phi(x)\}$ and $\phi(x) \ :\iff \ x \in B$.

Example 3.9. For $T : \mathcal{P}(\mathbb{R}^n) \to \mathcal{P}(\mathbb{R}^n)$ which closes under the vector operations (Example 3.4(b)), this says that to prove that a subset $B \subseteq \mathbb{R}^n$ contains the linear span of some vectors $\vec{v}_i$, it suffices to check that B contains each $\vec{v}_i$ and is itself a subspace.

For example, this is how one usually proves that $\operatorname{span}(A) \subseteq A^{\perp\perp}$, for every $A \subseteq \mathbb{R}^n$: clearly $A \subseteq A^{\perp\perp}$; and the orthogonal complement $B^\perp$ of every subset is a linear subspace.

Example 3.10. For $T : \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N})$ which closes under successor S (Example 3.4(f)), the T-closure of $A := \{0\}$ is all of $\mathbb{N}$. So the principle of T-induction says that to prove $\forall n \in \mathbb{N}\, \phi(n)$, it suffices to

- prove $\forall x \in \{0\}$, $\phi(x)$, i.e., $\phi(0)$;
- prove $\forall x \in \{y + 1 \mid \phi(y)\}$, $\phi(x)$, i.e., $\phi(y) \implies \phi(y + 1)$.

This is the ordinary principle of induction for $\mathbb{N}$.

For T which instead closes under 0 and S, the T-closure of $A = \varnothing$ is already all of $\mathbb{N}$. So to prove $\forall n \in \mathbb{N}\, \phi(n)$, it suffices to

- prove $\forall x \in \{0\} \cup \{y + 1 \mid \phi(y)\}$, $\phi(x)$, i.e., $\phi(0)$, and $\phi(y) \implies \phi(y + 1)$.

This is again the ordinary principle of induction for $\mathbb{N}$.

As this example indicates, considering the special case of $\overline{T}(\varnothing) = X$ is already enough in many cases. In fact, we can always reduce to this case; see Exercise 3.15 below. We thus restate the principle of induction in this special case, where it takes a simpler form:

Definition 3.11. We call a monotone set operator $T : \mathcal{P}(X) \to \mathcal{P}(X)$ **inductive** if $\overline{T}(\varnothing) = X$, i.e., the only T-closed subset of X is all of X.

Principle of T-induction for X. Let $T : \mathcal{P}(X) \to \mathcal{P}(X)$ be an inductive monotone set operator.

(a) For any $B \subseteq X$, if $T(B) \subseteq B$, then $B = X$.
(b) Equivalently, for any property $\phi(x)$, if $\forall x \in T(\{y \in X \mid \phi(x)\})$, $\phi(x)$, then $\forall x \in X$, $\phi(x)$.
(c) Equivalently, for any $\varnothing \neq C \subseteq X$, we have $C \cap T(X \setminus C) \neq \varnothing$.

Part (c) intuitively says that any nonempty $C \subseteq X$ contains an element which can be "derived" from elements not in C, and is equivalent to the contrapositive of (a) with $B := X \setminus C$.

Example 3.12. In the preceding example, we showed how taking $T : \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N})$ to close under $0, S$ yields the ordinary principle of induction.

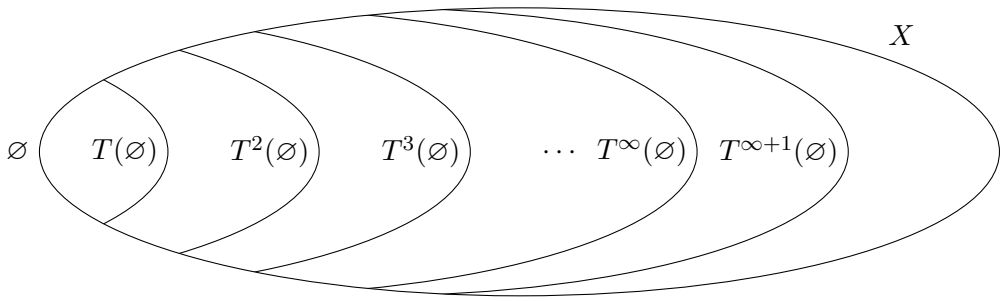
Taking instead $T(A) := \{n \in \mathbb{N} \mid \forall m < n\, (m \in A)\}$ as in Example 3.3, we get

(b) To prove $\forall n \in \mathbb{N}$, $\phi(n)$, it suffices to prove $\forall n \in \mathbb{N}$, $((\forall m < n,\, \phi(m)) \implies \phi(n))$. This is the *principle of strong induction* for $\mathbb{N}$.
(c) For any $\varnothing \neq C \subseteq \mathbb{N}$, there is $n \in C$ such that no $m < n$ is in C, i.e., n is the least element of C. This is the *well-ordering principle* for $\mathbb{N}$.

Remark 3.13. The proof of the Knaster–Tarski Theorem 3.6 is a "top-down" or (in philosophical terminology) *impredicative* construction: in order to build the *smallest* set obeying some condition, we had to look at *all possible* such sets. In other words, to build a simple thing, we had to look at everything more complicated than it. This is technique is very powerful, but a bit unsatisfying, since it tells us basically nothing about what the simple thing actually looks like.

A perhaps more satisfying "bottom-up" construction is to start with $\varnothing$ (nothing), then add everything derivable from that, yielding $T(\varnothing)$, then add everything derivable from that, yielding $T^2(\varnothing) = T(T(\varnothing))$, etc. After infinitely many steps, we're done if everything derivable from $T^\infty(\varnothing) := \bigcup_{n\in\mathbb{N}} T^n(\varnothing)$ can already be derived from a finite stage; this will be true if the notion of "derivation" defined by T is "finitary" in nature, e.g., if we're closing under finitary operations such as $+, \cdot$ in Example 3.4(a). If not, we have to keep going: $T^{\infty+1}(\varnothing) := T(T^\infty(\varnothing))$, etc.

(3.14)



But this description is only informal at this stage, because this "transfinite" process is an *instance* of the general inductive processes we're aiming to formalize; see Section 3.I.

Exercise 3.15. Let $T : \mathcal{P}(X) \to \mathcal{P}(X)$ be a monotone set operator, and fix $A \subseteq X$.

(a) Verify that $T_A(B) := A \cup T(B)$ is also a monotone set operator on X, restricting to $\overline{T}(A)$.
(b) Show that T_A is inductive on $\overline{T}(A)$, and that the principle of induction thereof yields the original principle of T-induction for $\overline{T}(A)$.
(c) Conclude that $\overline{T}(A) = A \cup T(\overline{T}(A))$.

3.B. **Examples of induction.** In this subsection, we assume we know about ordinary induction, and other basic facts, for $\mathbb{N}$, $\mathbb{R}$, etc. Our goal is to demonstrate the power of the general framework of induction, via some interesting examples from many different areas of math.

First, an amusing example of ordinary induction for $\mathbb{N}$:

Example 3.16 (blue-eyed islanders)**.** On an island live 500 inhabitants, 100 of whom have blue eyes while the other 400 have brown eyes. These islanders are extremely smart, able to immediately deduce any logically true statements. However, they have a very strict religion that forbids one from knowing one's own eye color; anyone who finds out their own eye color is required to commit ritual suicide the following day at noon in the village square, where all the other islanders can see. One day, a foreigner visits the island and casually remarks at a village gathering with everyone attending, "It's lovely to see another blue-eyed person like myself in this part of the world." What happens?

Solution. We claim that all of the blue-eyed people will simultaneously commit suicide 100 days after the foreigner makes the remark. More generally, we will prove by induction that if there are $n \geq 1$ blue-eyed people, they will all commit suicide n days after hearing the remark. If $n = 1$, the blue-eyed person finds out they have blue eyes, and so must commit suicide the next day. Now suppose the claim holds for n; we prove it for $n+1$. Each blue-eyed person sees n other blue-eyed people, hence knows there are either $n+1$ blue-eyed people in total (if they also have blue eyes) or n (if they don't). If there were n blue-eyed people, by the IH, they would commit suicide on the nth day. So on the nth day, since no one dies, every blue-eyed person figures out there are $n+1$ blue-eyed people, hence that they have blue eyes, hence must commit suicide on day $n+1$. □

Exercise 3.17. What happens to the brown-eyed people?

Exercise 3.18. What new information did the foreigner introduce that wasn't already known?

Exercise 3.19. Suppose one of the islanders is a noble saint, and would like to save everyone else. What can she do?

Remark 3.20. The philosophical/sociological/economic phenomenon this puzzle illustrates is known as *common knowledge*: everyone knows something, and everyone knows that everyone knows it, and everyone knows that everyone knows that everyone knows it, etc., which can be quite different than simply everyone knowing it. More complicated forms of induction can show up in common knowledge situations; see **TODO**.

We now turn to other forms of induction, i.e., other inductive set operators $T : \mathcal{P}(X) \to \mathcal{P}(X)$. In practice, one usually does not bother to explicitly write out the T; rather, one merely states the "closure" conditions, from which it is easy to read off T, as well as the principle of induction, which recall is equivalent to the assertion that T is inductive.

Proposition 3.21 (principle of Cauchy induction)**.** Let $f : \mathbb{N} \to \mathbb{N}$ be a strictly increasing function, i.e., $f(n) < f(n+1)$. Suppose $B \subseteq \mathbb{N}$ such that

- $f(0) \in B$;
- $f(n) \in B \implies f(n+1) \in B$;
- $n+1 \in B \implies n \in B$.

Then $B = \mathbb{N}$.

Proof. By ordinary induction, $f(n) \in B$ for every $n \in \mathbb{N}$. Since $0 \leq f(0) < f(1) < \cdots < f(n)$, $n \leq f(n)$ for all $n \in \mathbb{N}$ (technically, this is again by ordinary induction on n). By ordinary induction on k and the third property above, $n + k \in B \implies n \in B$. Thus for every $n \in \mathbb{N}$, from $f(n) = n + (f(n) - n) \in B$, we get $n \in B$. □

Exercise 3.22. What is the inductive set operator $T : \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N})$ for which the principle of T-induction yields the above?

Theorem 3.23 (AM–GM inequality)**.** For any $n \geq 1$ and $x_1, \ldots, x_n \in [0, \infty)$, we have

$$\frac{x_1 + \cdots + x_n}{n} \geq \sqrt[n]{x_1 \cdots x_n}.$$

Proof. By Cauchy induction with the increasing function $f(n) = 2^n$.

- For $n = 1$, it's trivially true: $x_1 \leq x_1$.
- For $n = 2$, expand $(\sqrt{x} - \sqrt{y})^2 \geq 0$ to get $x - 2\sqrt{xy} + y \geq 0$.
- Suppose it's true for 2^n; we prove it for 2^{n+1}.

$$\begin{aligned}
\frac{x_1 + \cdots + x_{2^{n+1}}}{2^{n+1}} &= \frac{\frac{x_1 + \cdots + x_{2^n}}{2^n} + \frac{x_{2^n+1} + \cdots + x_{2^{n+1}}}{2^n}}{2} \\
&\geq \frac{\sqrt[2^n]{x_1 \cdots x_{2^n}} + \sqrt[2^n]{x_{2^n+1} \cdots x_{2^{n+1}}}}{2} && \text{by IH} \\
&\geq \sqrt{\sqrt[2^n]{x_1 \cdots x_{2^n}} \sqrt[2^n]{x_{2^n+1} \cdots x_{2^{n+1}}}} && \text{by } n = 2 \text{ case} \\
&= \sqrt[2^{n+1}]{x_1 \cdots x_{2^{n+1}}}.
\end{aligned}$$

- Finally, suppose it's true for $n + 1$; we prove it for n. WLOG not every $x_i \neq 0$. Then

$$\begin{aligned}
\frac{x_1 + \cdots + x_n}{n} &= \frac{x_1 + \cdots + x_n + \frac{x_1 + \cdots + x_n}{n}}{n+1} \\
&\geq \sqrt[n+1]{x_1 \cdots x_n \left(\frac{x_1 + \cdots + x_n}{n}\right)} && \text{by IH.}
\end{aligned}$$

Raise to the $(n+1)$th power, divide by $\frac{x_1 + \cdots + x_n}{n} > 0$, and take the nth root. □

Definition 3.24. The **lexicographical ordering** on $\mathbb{N}^2$ is the binary relation defined as follows:

$$(a, b) <_{\text{lex}} (c, d) \iff (a < c) \text{ or } (a = c \ \&\ b < d).$$

Proposition 3.25 (principle of lexicographical induction on $\mathbb{N}^2$)**.** Let $B \subseteq \mathbb{N}^2$ such that

- for every $(a, b) \in \mathbb{N}^2$, if every $(c, d) <_{\text{lex}} (a, b)$ is in B, then $(a, b) \in B$.

Then $B = \mathbb{N}^2$.

Proof. We prove by (strong) induction on a that for every $a \in \mathbb{N}$, for every $b \in \mathbb{N}$, $(a, b) \in B$.

- Assume (IH) that for every $c < a$, for every $d \in \mathbb{N}$, $(c, d) \in B$. We now induct on b.
  - Assume (IH2) that for every $d < b$, $(a, d) \in B$. Then for every $(c, d) <_{\text{lex}} (a, b)$, either
    - $c < a$ in which case $(c, d) \in B$ by (IH), or
    - $c = a$ and $d < b$ in which case $(c, d) \in B$ by (IH2).

  Thus every $(c, d) <_{\text{lex}} (a, b)$ is in B, and so $(a, b) \in B$ by our assumption on B. □

Example 3.26 (Ackermann function)**.** Define the following computation on finite nonempty sequences of natural numbers, that takes a sequence and replaces the last two terms as follows:

$$\begin{aligned}
(a_0, \ldots, a_{n-1}, 0, y) &\longrightarrow (a_0, \ldots, a_{n-1}, y + 1), \\
(a_0, \ldots, a_{n-1}, x + 1, 0) &\longrightarrow (a_0, \ldots, a_{n-1}, x, 1), \\
(a_0, \ldots, a_{n-1}, x + 1, y + 1) &\longrightarrow (a_0, \ldots, a_{n-1}, x, x + 1, y).
\end{aligned}$$

For example:

$$\begin{aligned}
(1, 2) &\longrightarrow (0, 1, 1) \\
&\longrightarrow (0, 0, 1, 0) \\
&\longrightarrow (0, 0, 0, 1) \\
&\longrightarrow (0, 0, 2) \longrightarrow (0, 3) \longrightarrow (4).
\end{aligned}$$

Try starting with $(3, 3)$ instead. [Hint: if you're very fast, it'll take you around 2 hours.]

Theorem 3.27. This computation always terminates with a single term.

Proof. First, we prove that starting from any sequence $(a_0, \ldots, a_n, a_{n+1})$ with at least two terms, the computation eventually reaches some $(a_0, \ldots, b)$, by lexicographical induction on (a_n, a_{n+1}). Assume (IH) that this happens for every $(b_0, \ldots, b_m, b_{m+1})$ with $(b_m, b_{m+1}) <_{\text{lex}} (a_n, a_{n+1})$.

- If $a_n = 0$, we immediately get $(a_0, \ldots, a_{n+1} + 1)$.
- If $a_n > 0$ but $a_{n+1} = 0$, we get $(a_0, \ldots, a_n - 1, 1)$, which has the same length; since $(a_n - 1, 1) <_{\text{lex}} (a_n, 0)$, by the IH, we eventually reach some $(a_0, \ldots, b)$.
- If $a_n, a_{n+1} > 0$, we get $(a_0, \ldots, a_n - 1, a_n, a_{n+1} - 1)$ which has one more term, and by the IH eventually reaches some $(a_0, \ldots, a_n - 1, b)$; now since $(a_n - 1, b) <_{\text{lex}} (a_n, a_{n+1})$, this eventually becomes some $(a_0, \ldots, c)$.

Now by induction on n, every sequence of length $n > 0$ eventually reaches a single term. □

Remark 3.28. The Ackermann function $A : \mathbb{N}^2 \to \mathbb{N}$, that computes the single term above resulting from a pair of terms, is historically important as the first example of a function which can be computed by a program, but cannot be computed in a programming language that has only `if...else` clauses and loops of the form `for i = 0,...,n`. Such programs are called **primitive recursive**, and include virtually all algorithms used in the real world. (They include way more than commonly considered classes of functions in computational complexity theory, e.g., NP, EXPSPACE.)

Remark 3.29. In fact, since the above proof used lexicographical induction not to directly prove the claimed statement, but to prove an intermediate subclaim, the actual "length" of the induction of the entire proof is even "longer"; see **TODO**.

For a more general discussion of lexicographical induction, see Exercises 3.169 and 3.172.

Proposition 3.30 (real number induction)**.** Let $A \subseteq [0, \infty)$ (the nonnegative reals) such that

(i) $0 \in A$;
(ii) A is downward-closed, i.e., $y \le x \in A \implies y \in A$;
(iii) A is closed under increasing limits, i.e., if $x_0 < x_1 < \cdots \in A$ is bounded, then $\lim_{n\to\infty} x_n \in A$;
(iv) A is closed under $x \mapsto x + \varepsilon(x)$, for some fixed function $\varepsilon : [0, \infty) \to (0, \infty)$.

Then $A = [0, \infty)$.

Proof. We need to use Dedekind-completeness of $\mathbb{R}$: any nonempty subset A of $\mathbb{R}$ with an upper bound has a least upper bound $\sup A$. (This is a defining property of $\mathbb{R}$ that distinguishes it from $\mathbb{Q}$, that you would see in a real analysis course.) Suppose $A \neq [0, \infty)$. Then since A is downward-closed, any element of $[0, \infty) \setminus A$ is an upper bound for A. We also know $0 \in A$, so $\sup A$ exists. We must have $\sup A \in A$: if not, then $\sup A > 0$ (since $0 \in A$), and we can find a sequence $0 \le x_0 < x_1 \cdots < \sup A$ converging to $\sup A$ from below; since each $x_i < \sup A$, x_i is not an upper bound for A, hence is below some element of A, hence in A by downward-closure; but this contradicts (iii). But then $\sup A \in A$ is the greatest element of A, contradicting (iv). □

Theorem 3.31 (Heine–Borel)**.** Let $\mathcal{A}$ be a set of open intervals $(a, b) \subseteq \mathbb{R}$ such that $[0, 1] \subseteq \bigcup \mathcal{A}$. Then there is finite $\mathcal{F} \subseteq \mathcal{A}$ such that $[0, 1] \subseteq \mathcal{F}$.

Proof. We prove the same for $[0, x]$ in place of $[0, 1]$, by induction on x.

(i) For $x = 0$, $[0, 0] = \{0\}$ is contained a single interval in $\mathcal{A}$.
(ii) If finitely many intervals in $\mathcal{A}$ cover $[0, x]$, then they also cover $[0, y]$ for $y \le x$.
(iii) Let $x_0 < x_1 < \cdots \nearrow x < \infty$. Then x belongs to one interval $(a, b) \in \mathcal{A}$. Since $x_i \nearrow x$, there is n such that $x_n \in (a, b)$, whence $[x_n, x] \subseteq (a, b)$. By the induction hypothesis, there is finite $\mathcal{F} \subseteq \mathcal{A}$ covering $[0, x_n]$. Then $\mathcal{F} \cup \{(a, b)\}$ covers $[0, x]$.
(iv) For each $x \in [0, \infty)$, x belongs to an interval in $\mathcal{A}$, hence so does $x + 1/n$ for sufficiently large $n \in \mathbb{N}$; let $\varepsilon(x) := 1/n$ for the least such n. Then if finite $\mathcal{F} \subseteq \mathcal{A}$ covers $[0, x]$, then $\mathcal{F} \cup \{(a, b)\}$ for an interval (a, b) containing both $x, x + 1/n$ covers $[0, x + \varepsilon(x)]$. □

3.C. **Well-founded relations.** For a general monotone set operator $T : \mathcal{P}(X) \to \mathcal{P}(X)$, each $x \in T(A)$ may be "derivable" from A in more than one way, and there may not be a well-defined notion of "those $y \in A$ which are absolutely essential to derive x", i.e., a smallest $B \subseteq A$ such that $x \in T(B)$ (see Exercise 3.42 below). We now consider those special kinds of operators T for which there is always a set of such "essential predecessors" for each x. To specify such a set for each x is to give a function $X \to \mathcal{P}(X)$, which by the canonical bijection $\mathcal{P}(X)^X \cong \mathcal{P}(X \times X)$ (Exercise 2.82) is equivalently to give a binary relation on X.

Definition 3.32. Let $\prec \subseteq X^2$ ("precedes", `\prec` in TEX) be an arbitrary binary relation. The **induced monotone set operator** is

$$\begin{aligned} T = T_\prec : \mathcal{P}(X) &\longrightarrow \mathcal{P}(X) \\ A &\longmapsto \{x \in X \mid \forall y \prec x \, (y \in A)\} \\ &= \{x \in X \mid {\downarrow}x \subseteq A\} \end{aligned}$$

where

$${\downarrow}x = {\downarrow}_\prec x := \{y \in X \mid y \prec x\}$$

is the set of **$\prec$-predecessors** of x. We call $A \subseteq X$ **$\prec$-closed** if it is T-closed, i.e., if every $x \in X$ with ${\downarrow}x \subseteq A$ is itself in A. Thus, we also call $\overline{T}(A)$ the **T-closure** of A.

Remark 3.33. The $\downarrow$ notation is commonly used when $\prec$ is an ordering relation (see Definition 3.106). However, the definition makes sense for arbitrary $\prec$.

When $\prec$ is a reflexive partial order $\leq$, then ${\downarrow}x$ is often called the **downward closure** of x, or rather, of the singleton $\{x\}$. More generally, the **downward closure** of $A \subseteq X$ is

$$\begin{aligned} {\downarrow}A &= \{y \in X \mid \exists x \in A \, (y \leq x)\} \\ &= \{y \in X \mid \exists x \geq y \, (x \in A)\}. \end{aligned}$$

Note that T above is *not* the upward closure ${\uparrow}A$, defined the same way but with $\geq$ flipped to $\leq$! Rather, T is the *de Morgan dual*, with respect to set complement, of $\uparrow$:[11]

$$T(A) = X \setminus {\uparrow}(X \setminus A) = \{y \in X \mid \nexists x \prec y \, (x \notin A)\}.$$

Definition 3.34. We say that $\prec$ is a **well-founded** relation if the induced T is inductive, i.e.,

(a) We have the **principle of well-founded induction** for $\prec$: the only $\prec$-closed $B \subseteq X$ is X.
(b) Equivalently, to prove $\phi(x)$ for all x, it suffices to prove $\phi(x)$ assuming $\phi(y)$ for all $y \prec x$.
(c) Equivalently, every $\varnothing \neq C \subseteq X$ contains a **$\prec$-minimal** $x \in C$, i.e., $C \cap {\downarrow}x = \varnothing$.

More generally, the **well-founded part** of $\prec$ is $\mathrm{WF}(\prec) = \mathrm{WF}(X, \prec) := \overline{T}(\varnothing)$.

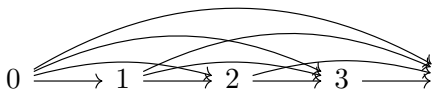
Example 3.35. On $\mathbb{N}$,

$$m \prec n \iff n = m + 1$$

defines a relation whose induced T is precisely that from Example 3.2, thus whose principle of well-founded induction is ordinary induction on $\mathbb{N}$. Here is a picture of this $\prec$:

$$0 \longrightarrow 1 \longrightarrow 2 \longrightarrow 3 \longrightarrow \cdots$$

Example 3.36. Still on $\mathbb{N}$, $\prec := <$ defines a relation whose induced T is that from Example 3.3, thus whose principle of well-founded induction is strong induction on $\mathbb{N}$. Picture:



[11] If $\prec$ were a reflexive partial order, then it would be consistent with terminology from topology to call $T(A)$ the **upward interior** of A (it is the interior operator of the topology whose closure operator is $\uparrow$). But this is too confusing in our context, where we want to think about *T-closure* for the purposes of induction.

As indicated by the above pictures, a common way to visualize an arbitrary binary relation R on a set X is as arrows or "directed edges" between the elements or "vertices". When thinking of R in this way, we also call it a **directed graph**, which is formally just a synonym for *binary relation*.

Definition 3.37. A binary relation $\prec \subseteq X^2$ is:

- **reflexive** if $x \prec x$ for all $x \in X$;
- **irreflexive** if $x \not\prec x$ for all $x \in X$;
- **symmetric** if $x \prec y \implies y \prec x$ for all $x, y \in X$;
- **antisymmetric** if $x \prec y \prec x \implies x = y$ for all $x, y \in X$;
- **transitive** if $x \prec y \prec z \implies x \prec z$ for all $x, y, z \in X$.

Note that "irreflexive" is not the same as "not reflexive", and "antisymmetric" is not the same as "not symmetric". Note also that given irreflexivity, antisymmetry is equivalent to: $x \not\prec y$ or $y \not\prec x$.

Proposition 3.38. A well-founded relation $\prec$ is irreflexive and antisymmetric, i.e., there are no **directed cycles** $x_0 \prec x_1 \prec \cdots \prec x_n = x_0$ of lengths $n = 1, 2$; in fact, there are no directed cycles of any length $n \geq 1$.

Proof. The directed cycle would be a subset with no minimal element. □

More generally, we have

Proposition 3.39. A binary relation $\prec \subseteq X^2$ is well-founded iff there are no infinite descending sequences $x_0 \succ x_1 \succ x_2 \succ \cdots$ (where $\succ := \prec^{-1}$). In other words, in the directed graph, there are no "paths from infinity" $\cdots \to x_2 \to x_1 \to x_0$.

Proof. $\implies$: Such a sequence would form a subset with no minimal element.

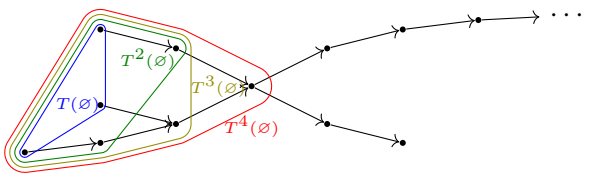
$\impliedby$: Suppose $\prec$ is not well-founded; let $C \subseteq X$ be nonempty with no minimal element. Pick $x_0 \in C$, then inductively, given $x_n \in C$ which cannot be minimal, pick $x_n \succ x_{n+1} \in C$. □

Remark 3.40. This might seem like a more intuitive definition of well-foundedness. However, from a foundational standpoint, the above proof is rather nontrivial: not only does it assume $\mathbb{N}$, i.e., the Axiom of Infinity, but it even uses the Axiom of Choice 3.203 in order to pick x_{n+1} arbitrarily from among the potentially many predecessors of x_n at each stage. (See Exercise 3.208.) This characterization is thus best used for visual intuition; the conceptual significance of well-foundedness is our official definition: that we can do induction on it.

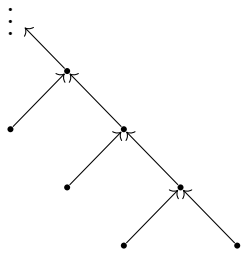
Example 3.41. A **simple undirected graph**, usually called simply a **graph**, is an irreflexive *symmetric* binary relation. Given an irreflexive antisymmetric $\prec$, we may symmetrize it into $\sim := \prec \cup \succ$. We may visualize this as vertices connected by *unoriented* edges (no arrows); the original $\prec$ amounts to picking one of the two possible orientations for each edge.

A graph $\sim$ is **acyclic** if it has no cycles of length ≥ 3. (Of course, any edge yields a cycle of length 2. There are no cycles of length 1, since we assumed irreflexivity.) An acyclic graph is also called a **forest**. A **tree** is a connected acyclic graph.

Note that if $\sim$ is a forest which is the symmetrization of an irreflexive antisymmetric $\prec$, then there are no instances of transitivity which hold for $\prec$, i.e., no x, y, z for which $x \prec y \prec z$ and also $x \prec z$, or else we would have a cycle of length 3. Example 3.35 is a tree (after symmetrizing); Example 3.36 is not, being transitive. Here is another example:



It is a bit silly to have "branches" of the tree pointing both backwards and forwards; usually, we would pick the orientations of the edges to point towards or away from a specified "root". Call $\prec$ a **directed forest** (some would say *coforest*) if it is irreflexive antisymmetric, its symmetrization is a forest in the above sense, and moreover each vertex x has at most one successor $y \succ x$. If x has no successor, it is a **root vertex** (of its connected component; some components may have no root vertex, in which case they are instead "rooted at infinity"). For example:



Exercise 3.42.

(a) Show that a binary relation $\prec \subseteq X^2$ may be recovered from the induced $T : \mathcal{P}(X) \to \mathcal{P}(X)$.

(b) Show that conversely, a monotone set operator $T : \mathcal{P}(X) \to \mathcal{P}(X)$ is induced by some binary relation $\prec$ iff T preserves arbitrary intersections, i.e., for any family of $A_i \subseteq X$, we have $T(\bigcap_i A_i) = \bigcap_i T(A_i)$ (keeping in mind Remark 2.21 about empty intersections); and that this is in turn equivalent to: for each $x \in X$, there is a smallest $A \subseteq X$ such that $x \in T(A)$. What is this smallest A, in terms of $\prec$?

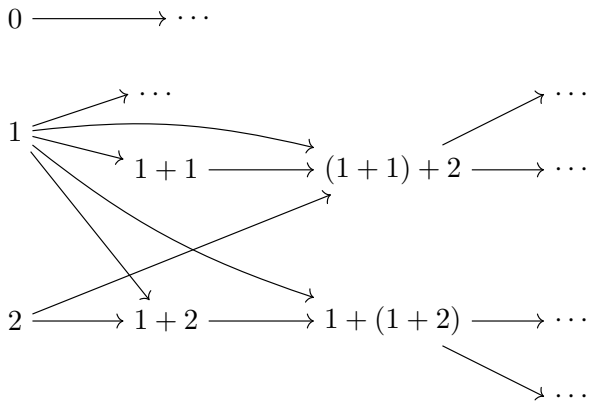
Thus, we have a bijection between the set of inductive monotone $T : \mathcal{P}(X) \to \mathcal{P}(X)$ preserving intersections, or equivalently such that each $x \in X$ may be "derived" from a smallest set, and the set of well-founded relations $\prec \subseteq X^2$.

Example 3.43. Closing under algebraic operations on some well-known structure does not typically correspond to a relation $\prec$. For example, $T : \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N})$ from Example 3.4 which closes under $+$ is not induced by any $\prec$, since it does not preserve intersections: we have $4 \in T(\{1,3\}) \cap T(\{2,2\})$, but $4 \notin T(\{1,3\} \cap \{2,2\}) = T(\varnothing) = \varnothing$.

However, if the set X consists of *formal symbolic expressions*[12] built from the operations f_i, then T does come from a well-founded $\prec$, namely

$$s \prec t \iff s \text{ is a immediate subexpression of } t = f_i(\dots, s, \dots) \text{ for some } f_i.$$

For example, if X consists of all expressions built from the single binary operation $+$, starting from the symbols $0, 1, 2$, then $\prec$ is given by a directed graph that looks like



[12] that is, terms in first-order logic

A key feature of notions of induction given by well-founded relations, that does *not* generalize (at least not easily; see Example 3.50 and Remark 3.51) to arbitrary monotone set operators, is that we may not only *prove* statements $\phi(x)$ by induction on x, but also *define* objects $f(x)$ inductively:[13]

Theorem 3.44 (principle of well-founded inductive definition)**.** Let $\prec$ be a well-founded relation on X, let $(Y_x)_{x\in X}$ be a family of sets, and let

$$\Big(F_x : \prod_{z\prec x} Y_z \to Y_x\Big)_{x\in X} \in \prod_{x\in X} Y_x^{\prod_{z\prec x} Y_z}.$$

Then there is a unique $f \in \prod_{x\in X} Y_x$ such that for each $x \in X$,

$$f(x) = F_x((f(z))_{z\prec x}).$$

In other words, "to define a family $(f(x) \in Y_x)_{x\in X}$, it suffices for each x to define $f(x) \in Y_x$ assuming given $f(z) \in Y_z$ for each $z \prec x$"; this definition of $f(x)$ given $(f(z))_{z\prec x}$ is given by F_x.

Proof. Uniqueness follows easily from well-founded induction: if $f, g \in \prod_{x\in X} Y_x$ are two such functions, and $f(z) = g(z)$ for all $z \prec x$, then

$$f(x) = F_x((f(z))_{z\prec x}) = F_x((g(z))_{z\prec x}) = g(x).$$

We now prove existence. We identify f with its graph, which is to be a set of pairs

$$f \subseteq \bigcup_{x\in X} (\{x\} \times Y_x) \subseteq X \times \bigcup_{x\in X} Y_x.$$

The requirement on f says that for each $x \in X$ and $y \in Y_x$,

$$(x, y) \in f \iff \exists (y_z)_{z\prec x} \in \textstyle\prod_{z\prec x} Y_z \,(y = F_x((y_z)_{z\prec x}) \;\&\; \forall z \prec x \,((z, y_z) \in f)).$$

By the Knaster–Tarski Theorem 3.6, there is such a set of pairs f. We prove that f is a function, i.e., $\forall x \in X \,\exists! y \in Y_x \,((x, y) \in f)$, by $\prec$-induction on x. Assume $\forall z \prec x \,\exists! y_z \, Y_z \,((z, y_z) \in f)$. Then by the above $\iff$, the unique y such that $(x, y) \in f$ is $y = F_x((y_z)_{z\prec x})$. □

Example 3.45. $! : \mathbb{N} \to \mathbb{N}$ (factorial), i.e., $(n!)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} \mathbb{N}$, is defined inductively as follows:

$$\begin{aligned} 0! &:= 0, \\ (n+1)! &:= (n+1) \cdot n!. \end{aligned}$$

In the above formalism: take $\prec$ to be the successor relation from Example 3.35, $X := Y_n := \mathbb{N}$, and

$$\begin{aligned} F_0 : \textstyle\prod_{m\in\downarrow 0} \mathbb{N} = \mathbb{N}^{\varnothing} &\longrightarrow \mathbb{N} \\ \varnothing &\longmapsto 0, \\ F_{n+1} : \textstyle\prod_{m\in\downarrow(n+1)} \mathbb{N} = \mathbb{N}^{\{n\}} &\longrightarrow \mathbb{N} \\ (y) &\longmapsto (n+1) \cdot y. \end{aligned}$$

Example 3.46. The Fibonacci sequence $(f(n))_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} \mathbb{N}$ is defined via *strong* induction:

$$\begin{aligned} f(0) &:= 0, \\ f(1) &:= 1, \\ f(n) &:= f(n-1) + f(n-2) \quad \text{for } n \geq 2. \end{aligned}$$

[13] Often, set theorists will insist that the correct terminology for "inductive definition" is **recursion**, and so the following should be called the *principle of well-founded recursion*; the term "induction" is reserved for proving statements. We think the term "inductive definition" is so well-used that this is a futile and pointless battle to fight.

In the above formalism: take $\prec := <$, $X := Y_n := \mathbb{N}$, and

$$F_n : \prod_{m<n} \mathbb{N} = \mathbb{N}^n \longrightarrow \mathbb{N}$$
$$(y_0, \ldots, y_{n-1}) \longmapsto \begin{cases} 0 & \text{if } n = 0, \\ 1 & \text{if } n = 1, \\ y_{n-1} + y_{n-2} & \text{if } n \geq 2. \end{cases}$$

Example 3.47. Recall the Ackermann function $A : \mathbb{N}^2 \to \mathbb{N}$ defined via an algorithm as in Example 3.26 and Remark 3.28. We may also define it directly, via lexicographical induction:

$$\begin{aligned} A(0, y) &:= y + 1, \\ A(x + 1, 0) &:= A(x, 1), \\ A(x + 1, y + 1) &:= A(x, A(x + 1, y)). \end{aligned}$$

Note that Example 3.26 is precisely the algorithm for expanding this definition:

$$\begin{aligned} A(1, 2) &= A(0, A(1, 1)) \\ &= A(0, A(0, A(1, 0))) \\ &= A(0, A(0, A(0, 1))) \\ &= A(0, A(0, 2)) = A(0, 3) = 4; \end{aligned}$$

now erase the A's and nested parentheses to recover the computation from Example 3.26.

In the formalism of Theorem 3.44: we use the lexicographical ordering $<_{\text{lex}}$ on $X := \mathbb{N}^2$ from Proposition 3.25, which says precisely that $<_{\text{lex}}$ is well-founded; $Y_{(x,y)} := \mathbb{N}$; and

$$\begin{aligned} F_{(0,y)} : \prod_{(u,v)<_{\text{lex}}(0,y)} \mathbb{N} = \mathbb{N}^{\{(0,0),\ldots,(0,y-1)\}} &\longrightarrow \mathbb{N} \\ \vec{a} &\longmapsto y + 1, \\ F_{(x+1,0)} : \prod_{(u,v)<_{\text{lex}}(x+1,0)} \mathbb{N} = \mathbb{N}^{(x+1)\times\mathbb{N}} &\longrightarrow \mathbb{N} \\ \vec{a} &\longmapsto a_{(x,1)}, \\ F_{(x+1,y+1)} : \prod_{(u,v)<_{\text{lex}}(x+1,y+1)} \mathbb{N} = \mathbb{N}^{((n+1)\times\mathbb{N})\cup\{(x+1,0),\ldots,(x+1,y)\}} &\longrightarrow \mathbb{N} \\ \vec{a} &\longmapsto a_{x,a_{x+1,y}}. \end{aligned}$$

Remark 3.48. In many examples, such as those above, the sets Y_x in Theorem 3.44 are the same. In fact, the general case where the Y_x's vary can be reduced to this simpler case, since we may take $Y := \bigcup_{x\in X} Y_x$, define $f : X \to Y$ inductively, and then prove by induction that in fact, each $f(x) \in Y_x$. On the other hand, the general form of Theorem 3.44 has the advantage that we may

Exercise 3.49. Deduce the principle of induction (i.e., that $\prec$ is well-founded) from the principle of inductive definition (Theorem 3.44).

Example 3.50. To see why the principle of inductive definition, unlike the principle of induction, only works for a well-founded relation $\prec$ rather than a general monotone $T : \mathcal{P}(X) \to \mathcal{P}(X)$: take

$$\begin{aligned} T : \mathcal{P}(\mathbb{N}) &\longrightarrow \mathcal{P}(\mathbb{N}) \\ A &\longmapsto \{0, 1\} \cup \{x + y \mid x, y \in A\}. \end{aligned}$$

This is clearly inductive. If we try to define a function $f : \mathbb{N} \to \mathbb{N}$ T-inductively via

$$\begin{aligned} f(0) &:= 0, \\ f(1) &:= 2, \\ f(x + y) &:= f(x)f(y), \end{aligned}$$

we get two inconsistent definitions $f(2) = f(1 + 1) = 2 \cdot 2 = 4$ and $f(2) = f(0 + 2) = 0 \cdot 4 = 0$.

Remark 3.51. Note, however, that if we changed the above to $f(0) := 1$, then we do get a consistent definition, namely $f(x) = 2^x$. Conceptually, this is because the 1 together with $\cdot$ on $\mathbb{N}$ form a *monoid*, i.e., an associative binary operation with an identity element. While $\mathbb{N}$ is not merely the set of all syntactic expressions built from $0, 1, +$ as in Example 3.43, it *is* the set of all such expressions quotiented by the monoid axioms (at least up to canonical bijection, e.g., $1 + 1 \sim 2 \sim 0 + (1 + 1)$), i.e., it's the *free monoid generated by* 1; the monoid axioms in some sense serve precisely to relate all the different, potentially conflicting ways in which each $x \in \mathbb{N}$ may be "derived" according to T. A similar idea applies to free groups (Definition 3.236), free rings (aka polynomial rings $\mathbb{Z}[X]$), etc.

3.D. **Homomorphisms and simulations.** Our goal for the next few subsections is, broadly speaking, to "compare" and "classify" different notions of induction. We will focus on well-founded relations, although some things can be generalized to inductive T, as indicated in Exercises.

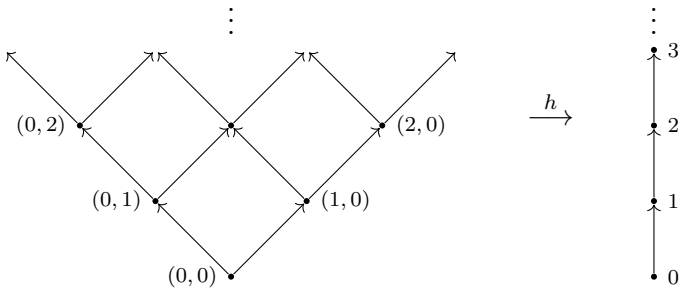
Example 3.52. Ordinary induction on $\mathbb{N}$ can clearly be "reduced" to strong induction. (The converse is true as well, of course; but there the reduction requires proof.)

What does this mean, precisely? The successor relation $\prec$ on $\mathbb{N}$ (Example 3.35) is a subgraph of the $<$ relation (Example 3.36), i.e., the predecessors $\downarrow_{\prec} x$ of the former are a subset of the precedessors $\downarrow_{<} x$ of the latter, for any $x \in \mathbb{N}$. Thus, if we know strong induction, then we can easily deduce ordinary induction, whose induction hypotheses are a subset of those for strong induction.

Example 3.53. Consider the following induction principle for $\mathbb{N}^2$: for $B \subseteq \mathbb{N}^2$, if

- $(0, 0) \in B$,
- $(0, y) \in B \implies (0, y + 1) \in B$,
- $(x, 0) \in B \implies (x + 1, 0) \in B$,
- $(x, y + 1), (x + 1, y) \in B \implies (x + 1, y + 1) \in B$,

then $B = \mathbb{N}^2$. This is induction for the following well-founded graph on the left:



We may prove this induction principle by proving that $(x, y) \in B$ for all $(x, y) \in \mathbb{N}^2$, by ordinary induction on $x + y$. In other words, we have the addition function $h : \mathbb{N}^2 \to \mathbb{N}$ which "reduces" this induction principle to ordinary induction for $\mathbb{N}$.

Definition 3.54. For two sets equipped with binary relations $(X, \prec_X)$ and $(Y, \prec_Y)$, a function $h : X \to Y$ is a **homomorphism** (between the relations) if for all $x, x' \in X$,

$$x' \prec_X x \implies f(x') \prec_Y f(x).$$

Proposition 3.55. For a homomorphism h as above, if $\prec_Y$ is well-founded, then so is $\prec_X$.

Proof idea. If $\prec_X$ is not well-founded, then (by Proposition 3.39) there is a descending sequence $x_0 \succ_X x_1 \succ_X \cdots$, whence $h(x_0) \succ_Y h(x_1) \succ \cdots$, whence $\prec_Y$ is not well-founded. □

However, we don't like this "proof" very much, for it uses not only $\mathbb{N}$ but also the Axiom of Choice! The following proof is similar in spirit, being based on the "contrapositive" form of the principle of induction. Below, we give another "forward" proof, generalizing the usual way that principles of induction may be used to prove each other (such as in Example 3.53).

Proof 1. If $\prec_X$ is not well-founded, then there is $\varnothing \neq C \subseteq X$ with no $\prec_X$-minimal element, whence $\varnothing \neq h[C] \subseteq Y$ has no $\prec_Y$-minimal element, since for every $h(x) \in h[C]$ where $x \in C$, there is $x' \prec_X x$, whence $h(x') \prec_Y h(x)$. □

Proof 2. Let $A \subseteq X$ be $\prec_X$-closed; we show that $\forall x \in X\,(x \in A)$, by $\prec_Y$-induction on $f(x)$. That is, we show that $\forall y \in Y\,\forall x \in f^{-1}(y)\,(x \in A)$, by $\prec_Y$-induction on y. Suppose (IH) this holds for all $y' \prec_Y y$. Then for all $x \in f^{-1}(y)$, for all $x' \prec_X x$, we have $f(x') \prec_Y f(x) = y$, whence by IH, $x' \in A$. Thus since A is $\prec_X$-closed, $x \in A$. □

Example 3.56. If $\prec$ is a well-founded relation on X, then any subrelation of $\prec$ is also well-founded (because id_X is a homomorphism). This covers Example 3.52.

Example 3.57. If $\prec$ is a well-founded relation on X, then for any $Y \subseteq X$, the restriction $\prec|Y := (\prec) \cap Y^2$ is well-founded on Y (because the inclusion $Y \hookrightarrow X$ is a homomorphism).

Exercise 3.58. Note that the above proof 2 of Proposition 3.55 uses the **coimage**

$$f\langle A\rangle := \{y \in Y \mid \forall x \in f^{-1}(y)\,(x \in A)\} = Y \setminus f[X \setminus A].$$

Generalize Proposition 3.55 to monotone set operators as follows: let X, Y be sets with monotone set operators T_X, T_Y respectively.

(a) Show that the following are equivalent:
  (i) For all $B \subseteq Y$, we have $f^{-1}[T_Y(B)] \subseteq T_X(f^{-1}[B])$.
  (ii) For all $A \subseteq X$, we have $T_Y(f\langle A\rangle) \subseteq f\langle T_X(A)\rangle$.
  (iii) For all $A \subseteq X$, we have $f[S_X(A)] \subseteq S_Y(f[A])$, where
  $$S_X(A) := X \setminus T_X(X \setminus A)$$
  is the de Morgan dual of T_X (we can think of $S_X(A)$ as those x which "depend on A", i.e., for which A is necessary, rather than sufficient, to derive x); similarly for S_Y.

(b) Show that if these hold, then they continue to hold when T_X, T_Y are replaced with $\overline{T_X}, \overline{T_Y}$.

(c) Conclude that $f^{-1}[\overline{T_Y}(\varnothing)] \subseteq \overline{T_X}(\varnothing)$. Thus, if T_Y is inductive, then so is T_X.

In fact, the notion of homomorphism is not the most natural or general way to compare well-founded relations. For example, in some cases, we want a function that transfers well-foundedness forwards rather than backwards.

Definition 3.59. For two sets equipped with binary relations $(X, \prec_X)$ and $(Y, \prec_Y)$, a relation $R \subseteq X \times Y$ is a **simulation** (of $\prec_X$ in $\prec_Y$) if for all $x, x' \in X$ and $y \in Y$,

$$x' \prec_X x\ R\ y \implies \exists y' \in Y\,(x'\ R\ y' \prec_Y y),$$

i.e.,

$$x\ R\ y \implies \forall x' \prec_X x\, \exists y' \prec_Y y\,(x'\ R\ y') \iff:\ x\ T_{\lesssim}(R)\ y,$$
$$R \circ (\prec_X) \subseteq (\prec_Y) \circ R.$$

We use squiggly arrows to denote R:

$$\begin{array}{ccc} x' & \xrightarrow{\prec_X} & x \\ R\,\vdots & & \vdots\,R \\ y' & \dashrightarrow_{\prec_Y} & y \end{array}$$

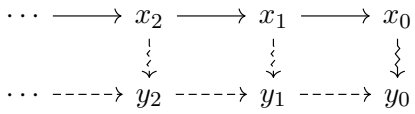
Example 3.60. If R is (the graph of) a function h, then this says precisely that h is a homomorphism (since y' must be $h(x')$). More generally, if R is only the graph of a partial function h, then this says that the domain of h must be $\prec_X$-downward-closed and that h is a homomorphism on its domain.

Example 3.61. $\leq$ is a simulation of $<$ on $\mathbb{N}$ in itself. Indeed, if $x' < x \leq y$, then there is y' (e.g., $y' = y - 1$) such that $x' \leq y' < y$.

The term "simulation" refers to "simulating the history of x's derivation", as in the following:

Proposition 3.62. For a simulation R with $\mathrm{dom}(R) = X$, if $\prec_Y$ is well-founded, then so is $\prec_X$. More generally, $R^{-1}[\mathrm{WF}(\prec_Y)] \subseteq \mathrm{WF}(\prec_X)$.

Bad proof idea.



□

Exercise 3.63. Give proofs using (a) every nonempty set has a minimal element; (b) induction.

Example 3.64. The addition homomorphism h from Example 3.53 is a simulation (being a homomorphism), and its inverse h^{-1} is also a simulation.

Definition 3.65. R is a **cosimulation** if R^{-1} is a simulation, and a **bisimulation** if it is both a simulation and a cosimulation, i.e.,

$$x\ R\ y \implies \forall x' \prec_X x\, \exists y' \prec_Y y\, (x'\ R\ y')\ \&\ \forall y' \prec_Y y\, \exists x' \prec_X x\, (x'\ R\ y') \iff:\ x\ T_{\approx}(R)\ y.$$

This intuitively means that x and y have "histories which look the same".

Corollary 3.66 (of Proposition 3.62)**.** If $h : X \twoheadrightarrow Y$ is a surjective cosimulation, and $\prec_X$ is well-founded, then so is $\prec_Y$. More generally, $h[\mathrm{WF}(\prec_X)] \subseteq \mathrm{WF}(\prec_Y)$. □

Proposition 3.67. Let $(X, \prec_X), (Y, \prec_Y), (Z, \prec_Z)$ be three sets with binary relations.

(a) $\mathrm{id}_X : X \to X$ is a (bi)simulation.
(b) If $R \subseteq X \times Y$ and $S \subseteq Y \times Z$ are (bi)simulations, then so is $S \circ R \subseteq X \times Z$.
(c) If $R \subseteq X \times Y$ is a bisimulation, then so is $R^{-1} \subseteq Y \times X$.

Proof. We only do (b): $S \circ R \circ (\prec_X) \subseteq S \circ (\prec_Y) \circ R \subseteq (\prec_Z) \circ S \circ R$; similarly for their inverses. □

Note that the definitions of *simulation* and *bisimulation* are both of the form "$R \subseteq T(R)$", for a suitable monotone set operator T as indicated above. This is dual to being T-closed.

Exercise 3.68 (dual Knaster–Tarski theorem)**.** Let $T : \mathcal{P}(X) \to \mathcal{P}(X)$ be a monotone set operator. Call $A \subseteq X$ **T-open** if $A \subseteq T(A)$. Show that for any $A \subseteq X$, there is a largest T-open $T^\circ(A) \subseteq A$, called the **T-interior** of A; and moreover, $T(T^\circ(X)) = T^\circ(X)$.

Definition 3.69. For sets with binary relations $(X, \prec_X), (Y, \prec_Y)$, define

$$(\lesssim) = (\lesssim_{X,Y}) := T^\circ_{\lesssim}(X \times Y) \subseteq X \times Y,$$
$$(\approx) = (\approx_{X,Y}) := T^\circ_{\approx}(X \times Y) \subseteq X \times Y.$$

These are the largest simulation and bisimulation between $\prec_X, \prec_Y$ respectively (and depend on $\prec_X, \prec_Y$, even though we don't write them in the notation). If $x \lesssim y$, we say x is **simulable** by y; if $x \approx y$, we say x, y are **bisimilar** (also known as *back-and-forth equivalent*).

By virtue of their definitions as the largest T-open sets for some T, we have:

$$x \lesssim y \iff x\ T_{\lesssim}(\lesssim)\ y \iff \forall x' \prec_X x\, \exists y' \prec_Y y\, (x' \lesssim y'), \tag{3.70}$$

$$x \approx y \iff x\ T_{\approx}(\approx)\ y \iff \forall x' \prec_X x\, \exists y' \prec_Y y\, (x' \approx y')\ \&\ \forall y' \prec_Y y\, \exists x' \prec_X x\, (x' \approx y'). \tag{3.71}$$

Principle of coinduction for $\lesssim, \approx$.

(3.72) If $x\ R\ y$ for some simulation R, then $x \lesssim y$.
(3.73) If $x\ R\ y$ for some bisimulation R, then $x \approx y$.

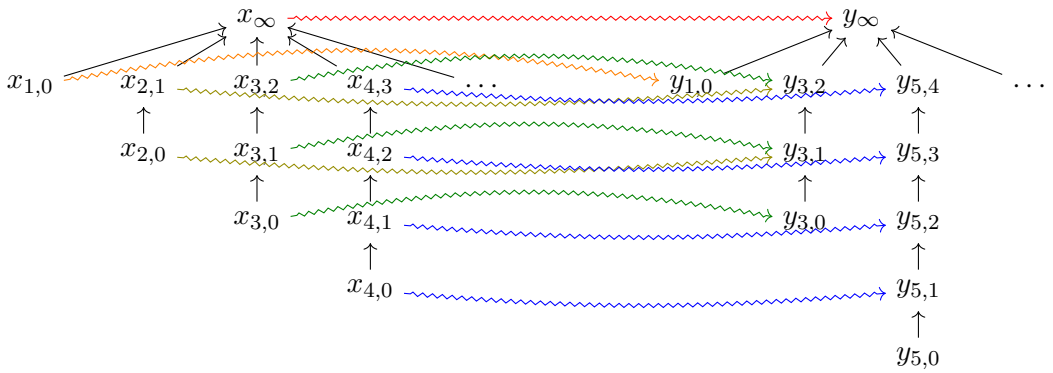
Proposition 3.74. If $x \simeq y$, then $x \lesssim y$ and $y \lesssim x$.

Proof. Because $\simeq$ is a simulation and a cosimulation, i.e., $\simeq^{-1}$ is a simulation. □

Example 3.75. If $x \in X$ has no predecessors, then it is simulable by all $y \in Y$, while it can only simulate $y \in Y$ which also has no predecessors, immediately by (3.70).

Thus, if $x \simeq y$, then x has no predecessors iff y does. Conversely, if x, y both have no predecessors, then clearly $x \simeq y$ (however, if both have predecessors, this may or may not hold).

Example 3.76. Let X, Y be the following well-founded trees:



We have a homomorphism $h : X \to Y$, thus also a simulation, shown in color, whence $x_\infty \lesssim y_\infty$. We also have a homomorphism $Y \to X$ mapping $y_{i,j} \mapsto x_{i,j}$, whence $y_\infty \lesssim x_\infty$.

However, we claim that $x_\infty \not\simeq y_\infty$. Otherwise, we would have (by (3.71)) $x_{2,1} \simeq y_{n,n-1} \prec_Y y_\infty$ for some n, whence $x_{2,0} \simeq y_{n,n-2} \prec_Y y_{n,n-1}$ (whence $n \geq 3$); but there is no $x' \prec_X x_{2,0}$ with $x' \simeq y_{n,n-3} \prec_Y y_{n,n-2}$.

Exercise 3.77. Which x in $(\mathbb{N}, <)$ are simulable by which y in $\mathbb{N}$ with the successor relation?

Corollary 3.78 (of Proposition 3.67)**.** Let $(X, \prec_X), (Y, \prec_Y), (Z, \prec_Z)$ be sets with binary relations.

(a) $x \simeq x$ for any $x \in X$.
(b) $x \simeq y \simeq z \implies x \simeq z$ and $x \lesssim y \lesssim z \implies x \lesssim z$ for $x \in X$, $y \in Y$, $z \in Z$.
(c) $x \simeq y \implies y \simeq x$ for $x \in X$, $y \in Y$.

Proof. For (b): $(\simeq_{Y,Z}) \circ (\simeq_{X,Y}) \subseteq X \times Z$ is a bisimulation by Proposition 3.67(b), hence contained in $(\simeq_{X,Z})$; similarly for $\lesssim$. □

3.E. **Extensionality and the Mostowski collapse.** The above three properties say that bisimilarity is an equivalence relation; in fact, not just on a single set with binary relation, but between all elements in all such sets. (Formally, it is an equivalence relation on $\bigsqcup_{(X,\prec)} X$, consisting of all triples $(X, \prec, x)$ where $\prec \subseteq X^2$ and $x \in X$, which is of course a proper class.)

Definition 3.79. A binary relation $\prec \subseteq X^2$ is **extensional** if $=_X$ is $T_\simeq$-closed, i.e.,

$$\begin{aligned} x \, T_\simeq(=_X) \, y &\iff \forall x' \prec x \, \exists y' \prec y \, (x' = y') \;\&\; \forall y' \prec y \, \exists x' \prec x \, (x' = y') \\ &\iff \forall z \in X \, (z \prec x \iff z \prec y) \\ &\iff {\downarrow}x = {\downarrow}y \implies x = y. \end{aligned}$$

Note that clearly, $(=_X) \subseteq T_\simeq(=_X)$; thus extensionality means $T_\simeq(=_X) = (=_X)$, i.e., $=_X$ is $T_\simeq$-closed. If it is in fact equal to $\simeq_{X,X}$, then we say $\prec$ is **strongly extensional**; since $\simeq$ is always reflexive, this equivalently means

$$x \simeq_{X,X} y \implies x = y.$$

Example 3.80. $\in$ is extensional, by the Axiom of Extensionality (2.1).

Example 3.81. If $\prec$ is extensional, it can have at most one minimal element (without predecessors). Thus for example, a typical directed forest is not extensional.

Example 3.82. Let $X = \{0, 1\}$, and let $\prec = (=_X)$:

This is extensional, since $\downarrow 0 \neq \downarrow 1$. However, it is not strongly extensional: $\{(0, 1)\}$ is a bisimulation (for the only predecessor $0 \prec 0$, there is $1 \prec 1$ such that $(0, 1) \in \{(0, 1)\}$), whence $0 \backsimeq 1$, but $0 \neq 1$.

Could $\in$ fail to be strongly extensional? Not in ZF; see Axiom 3.100.

Proposition 3.83. Let $\prec_X \subseteq X^2$ be well-founded, and $\prec_Y \subseteq Y^2$ be arbitrary. Then $\backsimeq_{X,Y}$ is the unique $T_\backsimeq$-fixed point in $\mathcal{P}(X \times Y)$.

Proof. By the bijection $\mathcal{P}(X \times Y) \cong \mathcal{P}(X)^Y$ (Exercise 2.82), a $T_\backsimeq$-fixed point R is determined by $R[\{x\}]$ for each $x \in X$; and to say R is $T_\backsimeq$-fixed means

$$x\ R\ y \iff \forall x' \prec x\, \exists y' \prec y\, (x'\ R\ y')\ \&\ \forall y' \prec y\, \exists x' \prec x\, (x'\ R\ y'),$$

i.e.,

$$R[\{x\}] = \{y \in Y \mid \forall x' \prec x\, \exists y' \prec y\, (y' \in R[\{x'\}])\ \&\ \forall y' \prec y\, \exists x' \prec x\, (y' \in R[\{x'\}])\},$$

whence $R[\{x\}]$ is uniquely defined by well-founded induction on x (Theorem 3.44). □

Corollary 3.84. A well-founded $\prec \subseteq X^2$ is extensional iff it is strongly extensional. □

Corollary 3.85. For a well-founded $\prec_X \subseteq X^2$, $\backsimeq_{X,Y}$ can also be defined as $\overline{T_\backsimeq}(\varnothing) \subseteq X \times Y$. □

Exercise 3.86. Show that for arbitrary $\prec_X, \prec_Y$:

(a) $\overline{T_\backsimeq}(\varnothing \subseteq X \times Y) = (\backsimeq_{X,Y}) \cap (\mathrm{WF}(\prec_X) \times Y) = (\backsimeq_{X,Y}) \cap (\mathrm{WF}(\prec_X) \times \mathrm{WF}(\prec_Y))$.

(b) $\overline{T_\backsimeq}(\varnothing \subseteq X^2) \cup (=_X) = \overline{T_\backsimeq}(=_X)$ is an equivalence relation on X.

Definition 3.87. The **strongly extensional quotient** of $(X, \prec_X)$ is the quotient set $X/{\backsimeq_{X,X}}$ equipped with the relation

$$\begin{aligned} D \prec_{X/\backsimeq_{X,X}} C &:\iff \forall x \in C\, \exists y \in D\, (y \prec_X x) \\ &\iff \exists x \in C\, \exists y \in D\, (y \prec_X x), \end{aligned}$$

where the choice of $x \in C$ is irrelevant because $\backsimeq$ is a bisimulation.

When $\prec_X$ is well-founded, we also call $X/{\backsimeq_{X,X}}$ simply the **extensional quotient**.

Proposition 3.88. The quotient map $X \twoheadrightarrow X/{\backsimeq_{X,X}}$ (mapping $x \mapsto [x]$) is a bisimulation.

Proof. It is a homomorphism using the "$\exists x \in C$" definition, and a cosimulation using "$\forall x \in C$".

$$\begin{array}{ccc} y & \xrightarrow{\prec_X} & x \\ {\scriptstyle\in}\,\vdots & & \vdots\,{\scriptstyle\in} \\ D & \xrightarrow{\prec_{X/\backsimeq_{X,X}}} & C \end{array}$$

□

Corollary 3.89 (of Proposition 3.62)**.** $\prec_X$ is well-founded iff $\prec_{X/\backsimeq_{X,X}}$ is. □

Corollary 3.90. $x \backsimeq_{X, X/\backsimeq_{X,X}} [x]$. □

Corollary 3.91. $[x] \backsimeq_{X/\backsimeq_{X,X}, X/\backsimeq_{X,X}} [y] \iff x \backsimeq_{X,X} y$. □

Corollary 3.92. $\prec_{X/\approx_{X,X}}$ is strongly extensional. □

Exercise 3.93. Show that in fact, $\approx_{X,X/\approx_{X,X}}$ is precisely the graph of the quotient map (i.e., $\in$).

We thus have a canonical procedure for "collapsing" bisimilar elements of *each* (well-founded) relation $\prec_X$. The question remains: can we somehow identify bisimilar elements across *all* (well-founded) relations? Note that there are proper class of them; thus the equivalence classes for the global $\approx$ relation are proper classes.[14] Nonetheless, note that for $x \in X$ (equipped with $\prec_X$) and $y \in Y$ (equipped with $\prec_Y$), we have

$$\begin{aligned} x \approx y &\iff \forall x' \prec x\, \exists y' \prec y\, (x' \approx y') \;\&\; \forall y' \prec y\, \exists x' \prec x\, (x' \approx y') \\ &\iff \forall x' \prec x\, \exists y' \prec y\, ([x'] = [y']) \;\&\; \forall y' \prec y\, \exists x' \prec x\, ([x'] = [y']) \\ &\iff \forall x' \prec x\, \text{“}[x'] \prec [y]\text{”} \;\&\; \forall y' \prec y\, \text{“}[y'] \prec [x]\text{”} \\ &\iff \text{“}\{[x'] \mid x' \prec x\} = \{[y'] \mid y' \prec y\}\text{”} \end{aligned}$$

(cf. Definition 3.79); the scare quotes are because we have not defined the $\prec$ relation on these proper equivalence classes $[x'], [y']$, nor may we collect them into these "meta-classes" on the last line. But this computation suggests that instead of collapsing bisimilar elements into an equivalence class, we can collapse them into these sets on the last line instead, which will indeed be sets, provided that all $x' \prec x$ have inductively likewise been collapsed into sets. This motivates

Definition 3.94. Let $\prec \subseteq X^2$ be a well-founded relation. The **Mostowski collapse** of $x \in X$ is defined inductively via

$$\twoheaddownarrow x = \twoheaddownarrow_{\prec} x := \{\twoheaddownarrow y \mid y \prec x\}.$$

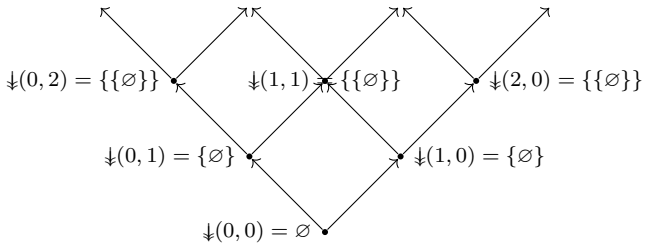
(Compare with $\downarrow x$ from Definition 3.32.) The **Mostowski collapse** of $(X, \prec)$ is $\twoheaddownarrow[X] = \{\twoheaddownarrow x \mid x \in X\}$.

Remark 3.95. There is a technical problem with this definition: we do not yet know that it exists! In the principle of well-founded inductive definitions stated thus far (Theorem 3.44), we need to assume given sets Y_x containing the values of the function $\twoheaddownarrow$ we're inductively defining. And this assumption is used in the proof of Theorem 3.44 via Knaster–Tarski, since we constructed the graph of the function as $\overline{T}(\varnothing) \subseteq \mathcal{P}(\bigsqcup_{x \in X} Y_x)$, which was constructed in the proof of Knaster–Tarski (Theorem 3.6) as the intersection of *all* T-closed subsets; we cannot take an intersection of all T-closed subclasses instead, since to define said intersection requires a $\forall$ over all such classes, which do not exist in the mathematical universe.

Note however that *provided* $\twoheaddownarrow$ can be defined as a (*a priori* proper) class, then it is in fact a set, by Replacement. Note also that we know $\twoheaddownarrow$ is unique if it exists, since the proof of the uniqueness part of Theorem 3.44 in that case is a simple well-founded induction on $\prec$.

Later in Theorem 3.119, we will give a different proof of well-founded inductive definition that *can* be generalized to proper classes. With this generalization, the above definition of $\twoheaddownarrow$ becomes perfectly valid. In the meantime, any results we prove about $\twoheaddownarrow$ should be interpreted as prefixed with "provided $\twoheaddownarrow$ exists".

Example 3.96. For the "grid" graph from Example 3.53:



[14] See however Corollary 3.199.

Proposition 3.97. For any well-founded relations $\prec_X \subseteq X^2$ and $\prec_Y \subseteq Y^2$, we have

$$x \approx_{X,Y} y \iff \downarrow x = \downarrow y.$$

Proof. By induction, we may assume this holds for all $x' \prec x$ (and all $y' \in Y$). Then

$$\begin{aligned} x \approx y &\iff \forall x' \prec x\, \exists y' \prec y\, (x' \approx y') \;\&\; \forall y' \prec y\, \exists x' \prec x\, (x' \approx y') \\ &\iff \forall x' \prec x\, \exists y' \prec y\, (\downarrow x' = \downarrow y') \;\&\; \forall y' \prec y\, \exists x' \prec x\, (\downarrow x' = \downarrow y') \quad \text{by IH} \\ &\iff \downarrow x = \{\downarrow x' \mid x' \prec x\} = \{\downarrow y' \mid y' \prec y\} = \downarrow y. \end{aligned}$$

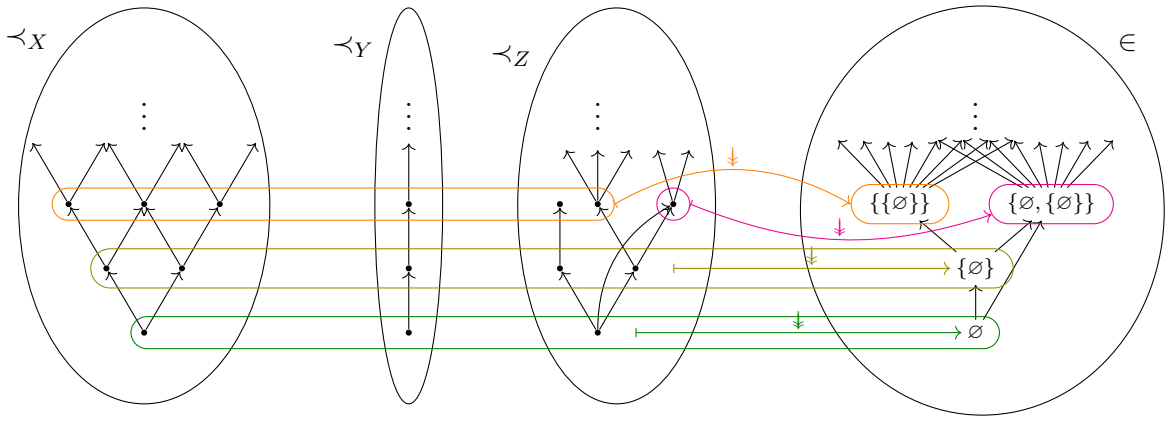
□

Corollary 3.98. For any well-founded $\prec \subseteq X^2$, $\downarrow : X \twoheadrightarrow \downarrow[X]$ is a bisimulation to $\in \subseteq \downarrow[X]^2$.

Proof. It is a homomorphism by definition: $x \prec y \implies \downarrow x \in \downarrow y$. To show that it is a cosimulation: if $\downarrow x \in \downarrow y$, then $\downarrow x = \downarrow z$ for some $z \prec y$; but by the preceding result, this means $x \approx z$. □

Exercise 3.99. Show that for any relation $\prec_X \subseteq X^2$ and strongly extensional relation $\prec_Y \subseteq Y^2$, $(\approx_{X,Y}) \subseteq X \times Y$ is a partial function. In particular, $\downarrow$ in the preceding corollary is unique.

We thus have a single "ultimate" notion of induction, namely the $\in$ relation between certain sets, to which all other notions of induction are bisimilar via the $\downarrow$ function:



(Colored blobs are $\approx$-classes.) Do we get *all* sets in this way, i.e., is $\in$ itself well-founded?

Axiom 3.100 (Foundation/Regularity)**.** For any set X, $\in_X \subseteq X^2$ is well-founded.

That is, for any $A \subseteq X$, if every $x \in X$ with $x \subseteq A$ is in A, then $A = X$.

Equivalently, every $\varnothing \neq C$ $(\subseteq X)$ contains a $\in$-minimal x, i.e., $x \cap C = \varnothing$.

Example 3.101. As a consequence of Foundation, there cannot be a set x such that $x \in x$, because then the singleton $\{x\}$ would not contain a $\in$-minimal element. (Thus the proper class $\{x \mid x \notin x\}$ in Russell's paradox (Corollary 2.10) is in fact the entire universe V.)

More generally, there cannot be any infinite descending sequences $x_0 \ni x_1 \ni \cdots$ (Proposition 3.39). *This says that the infinite sequence $(x_0, x_1, \dots)$ cannot exist (as a function from $\mathbb{N}$); it could still be the case that for each n individually, we can build a set x_n which lies in the previous one.*[15]

As this example shows, the precise connection between the Axiom of Foundation, and "true well-foundedness of $\in$", is a bit subtle; we will return to this topic in Section 3.J below.

Remark 3.102. People have occasionally considered alternatives to the Axiom of Foundation. One extreme example is *Aczel's Anti-Foundation Axiom*, which says "*every* binary relation $\prec \subseteq X^2$ has a unique Mostowski collapse". For instance, this implies "there is a unique x such that $x = \{x\}$", given by Mostowski collapsing the loop on a single vertex •↺ !

[15] For model theorists: it is easy to build a model of set theory, including Foundation, which externally has such an infinite descending sequence, using the compactness theorem for first-order logic.

3.F. **Transitivity.** We begin this subsection by tying up a loose end from the last. Under the Axiom of Foundation, arbitrary sets are precisely the representatives of bisimilarity classes of *elements* of sets with well-founded relations $(X, \prec)$, i.e., the Mostowski collapses $\downarrow\!\!\!\!\downarrow x$ of $x \in X$ (see Corollary 3.191 below). But which sets are the Mostowski collapses $\downarrow\!\!\!\!\downarrow[X]$ of the sets X themselves?

Example 3.103. $\{\{\varnothing\}\}$ is not $\downarrow\!\!\!\!\downarrow[X]$ for any set X equipped with a well-founded relation $\prec$. If it were, then $\{\varnothing\}$ would be $\downarrow\!\!\!\!\downarrow x$ for some $x \in X$; but then by definition of $\downarrow\!\!\!\!\downarrow x$, there must be $y \prec x$ with $\downarrow\!\!\!\!\downarrow y = \varnothing$ (i.e., $\downarrow y = \varnothing$), and so $\varnothing$ would also be in $\downarrow\!\!\!\!\downarrow[X]$.

Definition 3.104. Let $\prec \subseteq X^2$ be a binary relation. We say that $x \in X$ is **$\prec$-transitive** if

$$\forall z \prec y \prec x\, (z \prec x),$$
$$\text{or equivalently } \forall y \prec x\, (\downarrow y \subseteq \downarrow x).$$

Thus, $\prec$ is a transitive *relation* iff every $x \in X$ is a $\prec$-transitive *element*.

We say that a set X is **transitive** if it is $\in$-transitive, i.e., the following equivalent conditions:

$$\forall y \in x \in X\, (y \in X),$$
$$\forall x \in X\, (x \subseteq X),$$
$$X \subseteq \mathcal{P}(X).$$

Proposition 3.105. For a set X, the following are equivalent:

(i) X is a transitive set and $\in_X \subseteq X^2$ is well-founded (i.e., Foundation holds for X).
(ii) $\in_X$ is well-founded and $\downarrow\!\!\!\!\downarrow_{\in_X} = \mathrm{id}_X$.
(iii) $\in_X$ is well-founded and $X = \downarrow\!\!\!\!\downarrow_{\in}[X]$.
(iv) $X = \downarrow\!\!\!\!\downarrow_{\prec}[Y]$ for some well-founded relation $\prec \subseteq Y^2$.
(v) $X = \downarrow\!\!\!\!\downarrow_{\prec} y$ for some well-founded relation $\prec \subseteq Y^2$ and $\prec$-transitive element $y \in Y$.

Proof. (i) $\Longrightarrow$ (ii): Note that id_X obeys the inductive definition (3.94) of $\downarrow\!\!\!\!\downarrow$.
(ii) $\Longrightarrow$ (iii) $\Longrightarrow$ (iv) is obvious.
(iv) $\Longrightarrow$ (v): Let $\top$ be a new element not in Y,[16] and put $y \prec \top$ for all $y \in Y$; then $\downarrow\!\!\!\!\downarrow[Y] = \downarrow\!\!\!\!\downarrow\top$.
(v) $\Longrightarrow$ (i) is obvious from the definitions of $\downarrow\!\!\!\!\downarrow$ and transitivity. □

We now turn to transitivity of relations, which is the other way of "comparing" different notions of induction. Bisimilarity is a "horizontal" comparison: it only relates elements which have "identical histories", regardless of how "long" those histories are. But for instance, the successor relation on $\mathbb{N}$ and the $<$ relation (Example 3.52) are not bisimilar (since a bijective bisimulation must be an isomorphism), even though they intuitively have the same "length" (cf. Exercise 3.77).

Definition 3.106. A binary relation is an **irreflexive partial order** (or **strict partial order**) if it is irreflexive, transitive, and antisymmetric, and a **reflexive partial order** if it is reflexive, transitive and antisymmetric. It is easily seen that for any set X, we have a bijection

$$\{\text{irreflexive partial orders } < \subseteq X^2\} \cong \{\text{reflexive partial orders } \leq \subseteq X^2\}$$
$$< \mapsto < \cup (=_X)$$
$$\leq \setminus (=_X) \mapsfrom \leq.$$

By **partial order**, we ambiguously mean either of these, depending on context; when we have a $<$ or $\leq$, by default we always use the other symbol to denote its (pre)image under this bijection.

An **irreflexive linear order** (or *total order*) $<$ is an irreflexive partial order which moreover satisfies **trichotomy**

$$\forall x, y \in X\, (x < y \text{ or } x = y \text{ or } y < x).$$

[16] Under Foundation, we may take $\top := Y$; regardless, Russell's paradox says that $\top := \{y \in Y \mid y \notin y\}$ works.

For a **reflexive linear order** $\leq$, this is equivalent to **dichotomy**

$$\forall x, y \in X\,(x \leq y \text{ or } y \leq x).$$

Again, a **linear order** means either of these.

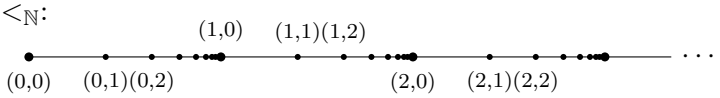
A **well-order** is a well-founded irreflexive linear order. Since well-foundedness necessarily implies irreflexivity (Proposition 3.38), when we say e.g., "$\leq$ is a well-order", we really mean that $<$ is. Similarly, a **partial well-order** is a well-founded irreflexive partial order, or equivalently just a well-founded transitive relation (since well-foundedness implies irreflexivity and antisymmetry).

Exercise 3.107. Show that a well-founded relation obeying trichotomy is automatically transitive.

Definition 3.108. The **transitive closure** of an arbitrary binary relation $\prec \subseteq X^2$ is the smallest transitive relation containing it (which exists by Knaster–Tarski; cf. Example 3.5).

Example 3.109. $<$ is a well-order on $\mathbb{N}$, and is the transitive closure of the successor relation.

Example 3.110. $<_{\text{lex}}$ is a well-order on $\mathbb{N}^2$ (well-foundedness is by Proposition 3.25), which is much "longer" than $<_{\mathbb{N}}$:



Example 3.111. The transitive closure of the "grid" in Example 3.53 is the partial well-order

$$(a, b) < (c, d) \;:\iff\; a \leq c \;\&\; b \leq d \;\&\; (a < c \text{ or } b < d)$$

(which is well-founded again because addition $h : \mathbb{N}^2 \to \mathbb{N}$ is a homomorphism, now to $<$).

Exercise 3.112. Assuming ordinary induction on $\mathbb{N}$, show that the transitive closure of $\prec$ is

$$x < y \;:\iff\; \exists n \geq 1\, \exists x = x_0 \prec x_1 \prec \cdots \prec x_{n-1} \prec x_n = y.$$

Proposition 3.113. Let $\prec \subseteq X^2$ be a binary relation. The transitive closure $<$ of $\prec$ is the smallest binary relation containing $\prec$ such that

$$(*) \qquad x \prec y < z \implies x < z.$$

In other words, for each $z \in X$, $\downarrow_< z \subseteq X$ is the $\prec$-downward-closure of $\downarrow_\prec z$.

Note the significance of this: by definition, $<$ is the smallest relation containing $\prec$ such that

$$x < y < z \implies x < z;$$

since $<$ occurs twice on the LHS, with two different RHSs, the induction principle for $<$ tells us how to prove that $x < y$ implies another property $\phi(x, y)$ of two variables. By contrast, because $(*)$ only involves $<$ with a *single* RHS, we may define each of the "horizontal cross-sections" $\downarrow_< z$ of $<$ separately; thus we get an induction principle to show that $x < z$ implies $\phi(x)$ *for fixed* z.

Proof idea. This is rather obvious using Exercise 3.112. But we don't want to use $\mathbb{N}$ yet! □

Proof. The smallest such $<$ is contained in the transitive closure of $\prec$, since the latter is clearly also a binary relation satisfying $(*)$. Thus it remains to show that $<$ contains the transitive closure of $\prec$; since $<$ contains $\prec$ by definition, it suffices to show that $<$ is already transitive, i.e.,

$$\forall x < y \underbrace{\forall z \in X\,(y < z \implies x < z)}_{\phi(x,y)}.$$

We induct on $x < y$, i.e., we show that the set of (x, y) satisfying ϕ also contains $\prec$ and obeys $(*)$. Indeed, $x \prec y \implies \phi(x, y)$ since $<$ satisfies $(*)$ by definition. And we have

$$\begin{aligned} x \prec y \;\&\; \phi(y, z) &\iff x \prec y \;\&\; \forall w \in X\,(z < w \implies y < w) \\ &\implies \forall w \in X\,(z < w \implies x < w) \iff \phi(x, z) \quad \text{by } (*). \end{aligned}$$

□

Corollary 3.114. The transitive closure $<$ of $\prec$ is also the smallest relation containing $\prec$ such that

$$x < y \prec z \implies x < z.$$

Proof. Either copy the above proof, or apply the above result to $\succ$. □

Proposition 3.115. Let $\prec \subseteq X^2$ be a binary relation with transitive closure $<$ (which may or may not be irreflexive, if $\prec$ is not well-founded), and $\leq := < \cup (=_X)$. Then $\leq$ is a simulation from $<$ to $\prec$ (while id_X is a homomorphism in the reverse direction). In particular, every $x \in X$ simulates itself from $\prec$ to $<$ and vice-versa; hence $\mathrm{WF}(\prec) = \mathrm{WF}(<)$, and $\prec$ is well-founded iff $<$ is.

Recalling again that for $\prec :=$ the successor relation on $\mathbb{N}$, equality is not a *bisimulation* between $\prec$ and $<$, this gives yet another illustration of the difference between mutual simulability in both directions $\lesssim \cap \gtrsim$ and bisimilarity $\backsimeq$ (cf. Example 3.76).

Proof. Let $x' < x \leq y$; then either $x = y$ or $x < y$, both of which yield $x' < y$.

$$\begin{array}{ccc} x & \overset{\leq}{\rightsquigarrow} & y \\ {\scriptstyle <}\uparrow & & \uparrow{\scriptstyle \prec} \\ x' & \overset{\leq}{\rightsquigarrow} & y' \end{array}$$

By Corollary 3.114 and Exercise 3.15, we have $< \; = \; \prec \cup (\prec \circ <) \; = \; \prec \circ \leq$; thus $x' < y$ means $x' \leq y' \prec y$ for some y'. □

Corollary 3.116. Let $\prec_X \subseteq X^2$ and $\prec_Y \subseteq Y^2$, with transitive closures $<_X, <_Y$ respectively. Then $\lesssim_{X,Y}$ between $\prec_X, \prec_Y$ is the same as between $<_X, <_Y$.

Proof. Because we can compose the simulations $\lesssim_{X,Y}$ with $\lesssim, \gtrsim$ between $\prec, <$:

$$\begin{array}{ccc} (X, \prec_X) & \overset{\lesssim_{X,Y}}{\rightsquigarrow} & (Y, \prec_Y) \\ {\scriptstyle \mathrm{id}_X \subseteq (\lesssim \cap \gtrsim)}\downarrow & & \downarrow{\scriptstyle \mathrm{id}_Y \subseteq (\lesssim \cap \gtrsim)} \\ (X, <_X) & \overset{\lesssim_{X,Y}}{\rightsquigarrow} & (Y, <_Y) \end{array}$$

□

Exercise 3.117. Give a direct proof that $\prec$ is well-founded iff its transitive closure $<$ is. [Imitate the usual proof of strong induction from ordinary induction on $\mathbb{N}$: to prove $\forall n\, \phi(n)$ by strong induction, prove $\forall n \forall m \leq n\, \phi(n)$ by ordinary induction. You'll probably need a step similar to the use of Corollary 3.114 and Exercise 3.15 above.]

Exercise 3.118. Let $T : \mathcal{P}(X) \to \mathcal{P}(X)$ be a monotone set operator. We say T is **transitive** if $T(A) \subseteq T(T(A))$ for every $A \subseteq X$.

(a) Show that $T = T_\prec$ for $\prec \subseteq X^2$ (recall Definition 3.32) is transitive iff $\prec$ is.
(b) Show that $T^\circ \circ T$ is transitive and pointwise $\subseteq T$, meaning $(T^\circ \circ T)(A) \subseteq T(A)$ for all A. Moreover, it is the pointwise largest such monotone set operator.
(c) Show that $T^\circ_\prec \circ T_\prec = T_<$, where $<$ is the transitive closure of $\prec$.
(d) Show that $\overline{T}(\varnothing) = \overline{T^\circ \circ T}(\varnothing)$. [Show $\overline{T^\circ \circ T}(\varnothing) \subseteq T(\overline{T^\circ \circ T}(\varnothing))$, and apply T.]
(e) Deduce the preceding exercise.

One important application of transitivity is a more powerful version of the principle of well-founded inductive definition from Theorem 3.44. In that previous version, we needed to provide codomain *sets* Y_x into which the function we are defining maps; as noted in Remark 3.95, such a restriction was necessary in the proof we gave via Knaster–Tarski, but is inconvenient in some cases when we are trying to inductively define objects in the universe outside of any sets we start with. We may now remove this restriction, by giving a different proof:

Theorem 3.119 (principle of well-founded inductive definition, unbounded codomain version)**.** Let $\prec$ be a well-founded relation on a set X, let $(Y_x)_{x\in X}$ be a family of *classes*, or more precisely a single class relation (class of pairs) Y with $Y_x := Y[\{x\}]$, and let

$$\left(F_x : \prod_{z\prec x} Y_z \to Y_x\right)_{x\in X}$$

be a family of functions, or more precisely a single class function $F(x,\vec{y})$. Then there is a unique $f \in \prod_{x\in X} Y_x$ such that for each $x \in X$,

$$(*) \qquad f(x) = F_x((f(z))_{z\prec x}).$$

Proof. The proof of uniqueness from Theorem 3.44 still works.

For existence, first suppose $\prec$ is a partial well-order $<$. Note then that for any $x \in X$, $\downarrow_{\leq} x \subseteq X$ is $<$-downward-closed, and so the function f satisfying $(*)$ we are trying to define will restrict to the function defined inductively via the same $(F_z)_{z\leq x}$ on $(\downarrow_{\leq} x, \prec|\downarrow_{\leq} x)$; moreover, to compute $f(x)$, it suffices to know such a restriction $f|\downarrow_{\leq} x$.

We thus prove by $<$-induction that for each $x \in X$, there is a (unique, as shown before) function $f_x \in \prod_{z\leq x} Y_z$ satisfying $(*)$. Assume such $f_z \in \prod_{w\leq z} Y_w$ exist for every $z < x$. Then $\bigcup_{z<x} f_z$ is a function on $\downarrow_{<} x$, since for two $z, z' < x$, both $f_z, f_{z'}$ restrict to the same function on $\downarrow_{\leq} w$ (by uniqueness) for every $w \leq z, z'$, whence $f_z(w) = f_{z'}(w)$. Moreover, $\bigcup_{z<x} f_z \in \prod_{z<x} Y_z$ satisfies $(*)$, since every f_z does. Now extend this to $f_x \in \prod_{z\leq x} Y_z$ by defining $f_x(x)$ according to $(*)$; this completes the induction. Finally, take $f := \bigcup_{x\in X} f_x$; this is a function for the same reason as before.

If $\prec$ is merely a well-founded relation, apply the above to its transitive closure $<$. □

Proposition 3.115 clarifies the nature of the one-way simulability relation $\lesssim$: it contains at least the reflexive transitive closure $\leq$ of the underlying relation $\prec$. Clearly, $\lesssim$ also contains the bisimilarity relation $\eqsim$. Moreover, by Corollary 3.116, we may understand $\lesssim$ for general $\prec$ in terms of $\lesssim$ for the transitive closure $<$. We will show (see Corollary 3.126) that $\lesssim$ on a partial well-order $<$ is just the composition of $\leq$ and $\eqsim$; hence, $\lesssim$ between general well-founded relations is the composition of reflexive transitive closure and bisimilarity.

Proposition 3.120. For an irreflexive linear order $< \subseteq X^2$, we have $T_{\lesssim}(\leq) = \leq$.

Proof. $\supseteq$ by Proposition 3.115. Now suppose $x\, T_{\lesssim}(\leq)\, y$, i.e., every $x' < x$ is $\leq y' < y$ for some y'. If $x \not\leq y$, then by linearity, $x > y$, whence $y \leq y' < y$ for some y', contradicting irreflexivity. □

Exercise 3.121 (cf. Proposition 3.83)**.** Let $\prec_X \subseteq X^2$ and $\prec_Y \subseteq Y^2$, with at least one well-founded. Then $\lesssim_{X,Y}$ is the unique $T_{\lesssim}$-fixed point in $\mathcal{P}(X \times Y)$.

Proposition 3.122. Let $< \subseteq X^2$ be a partial well-order. The following are equivalent:

(i) $<$ is linear, i.e., a well-order.
(ii) $<$ is (strongly) extensional, i.e., $(\eqsim_{X,X}) = (=_X)$.
(iii) $(\lesssim_{X,X} \cap \gtrsim_{X,X}) = (=_X)$.
(iv) $(\lesssim_{X,X}) = (\leq)$.

Proof. (ii) $\Longrightarrow$ (i): We prove every $x \in X$ is comparable with every $y \in X$, by induction on x. Assume (IH1) every $x' < x$ is comparable with every $y \in X$. We now induct on y: assume (IH2) every $y' < y$ is comparable with x. If some $y' < y$ is $\geq x$, then $x \leq y' < y$ so we're done. Otherwise, every $y' < y$ is $< x$, i.e., $\downarrow_{<} y \subseteq \downarrow_{<} x$. Similarly, if some $x' < x$ is $\geq y$, then $y \leq x' < x$ so we're done. In the remaining case, we have $\downarrow_{<} x = \downarrow_{<} y$, so $x = y$ by extensionality.

(i) $\Longrightarrow$ (iv) by the two preceding results; (iv) $\Longrightarrow$ (iii) $\Longrightarrow$ (ii) are obvious. □

Exercise 3.123. Which implications above still hold in the absence of well-foundedness?

Proposition 3.124. Let $<_X \subseteq X^2$ and $<_Y \subseteq Y^2$ be two well-orders.

(a) $\simeq_{X,Y} \subseteq X \times Y$ is a partial isomorphism, either between X and an initial (i.e., $<_Y$-downward-closed) segment of Y, or between an initial segment of X and all of Y.
(b) $(\lesssim_{X,Y} \cap \gtrsim_{X,Y}) = (\simeq_{X,Y})$.
(c) $(\lesssim_{X,Y}) = (\leq_Y \circ \simeq_{X,Y})$, i.e., $x \lesssim_{X,Y} y \iff \exists y' \, (x \simeq_{X,Y} y' \leq y) \iff \simeq_{X,Y}(x) \leq y$.

Proof. (a) Its domain and codomain are initial segments by definition of bisimulation, it is a partial bijection by Exercise 3.99, and a partial isomorphism because it is a bisimulation. If there were both some $x \in X \setminus \mathrm{dom}(\simeq_{X,Y})$ and some $y \in Y \setminus \mathrm{rng}(\simeq_{X,Y})$, then taking the least such x, y, we would have $\forall x' < x \, \exists y' < y \, (x' \simeq y')$ (namely the unique such y', since $x' \in \mathrm{dom}(\simeq_{X,Y})$), and similarly vice-versa, whence $x \simeq y$, a contradiction.

(c) $\supseteq$ because the RHS is a simulation (using Proposition 3.115 for $\leq_Y$). Conversely, suppose $x \lesssim_{X,Y} y$. If $x \in \mathrm{dom}(\simeq_{X,Y})$, then letting $x \simeq y'$, we have $y' \simeq x \lesssim y$, whence $y' \lesssim y$, whence $y' \leq y$ by Proposition 3.122. Otherwise, by (a), we instead have some $x' \simeq y$; but then we similarly get $x \lesssim y \simeq x' \implies x \leq x'$, a contradiction since $\mathrm{dom}(\simeq_{X,Y})$ must be an initial segment of X.

(b) follows easily from (c). □

Proposition 3.125. Let $< \subseteq X^2$ be transitive. Then the induced relation $<_{X/\simeq}$ on the strongly extensional quotient as in Definition 3.87 is also transitive, hence a well-order if $<$ was well-founded.

Proof. If $C <_{X/\simeq} D <_{X/\simeq} E$, then for every $z \in E$, there is $y \in D$ with $y < z$, and then there is $x \in C$ with $x < y$, whence $x < y < z$, which shows $C < E$. □

Corollary 3.126. Let $<_X \subseteq X^2$ and $<_Y \subseteq Y^2$ be two partial well-orders.

(b) $(\lesssim_{X,Y} \cap \gtrsim_{X,Y}) = (\simeq_{X,Y})$.
(c) $(\lesssim_{X,Y}) = (\leq_Y \circ \simeq_{X,Y})$, i.e., $x \lesssim_{X,Y} y \iff \exists y' \, (x \simeq_{X,Y} y' \leq y)$.

Proof. (b) follows from Proposition 3.124(b) and $x \simeq [x]$ (Proposition 3.88).

(c) similarly follows from Proposition 3.124(c), via a diagram chase:

$$\begin{array}{ccccccc} x & \in & X & \rightsquigarrow & Y & \ni & y \\ \downarrow & & \updownarrow & & \updownarrow & & \downarrow \\ [x] & \in & X/\simeq & \rightsquigarrow & Y/\simeq & \ni & [y] \end{array}$$

If $x \lesssim_{X,Y} y$, then $[x] \simeq x \lesssim y \simeq [y]$ (3.88), whence there is $[x] \simeq D \leq [y]$ by Proposition 3.124(c), whence there is $y' \in D$ such that $y' \leq y$ (3.87), whence $x \simeq [x] \simeq D \simeq y'$. □

Exercise 3.127. Find transitive non-well-founded relations for which (b) above fails.

Definition 3.128. The **well-ordered quotient** of a well-founded $\prec \subseteq X^2$ is the extensional quotient of the transitive closure $<$; we denote it by $X/\lesssim_{X,X}$ (due to Corollary 3.131 below).

This combines the two methods of "simplifying" a well-founded relation we have discussed:

$$\begin{array}{lccc} \text{arbitrary well-founded} & (X, \prec) & \xrightarrow[\lesssim \cap \gtrsim]{\mathrm{id}_X} & (X, <) \quad \text{transitive} \\ & \simeq \downarrow & & \downarrow \simeq \\ \text{extensional} & (X/\simeq, \prec) & \overset{(3.132)}{\dashrightarrow} & (X/\lesssim, <) \quad \text{well-order} \end{array}$$

Corollary 3.129. The quotient map $(X, \prec) \twoheadrightarrow (X/\lesssim, <)$ is contained in $\lesssim \cap \gtrsim$.

Proof. id_X is by Proposition 3.115; the right quotient map is a bisimulation by Proposition 3.88. □

Corollary 3.130. For well-founded $\prec_X, \prec_Y$, we have $[x] \lesssim_{X/\lesssim, Y/\lesssim} [y] \iff x \lesssim_{X,Y} y$. □

Corollary 3.131. $X/\lesssim$ is also the quotient of X by $\lesssim \cap \gtrsim$. □

Corollary 3.132. The quotient map $(X, \prec) \twoheadrightarrow (X/\lesssim, <)$ descends to $(X/\eqsim, \prec)$. □

Exercise 3.133. Give an example where this descended map is not a bijection, i.e., where $\eqsim$ on $(X, <)$ is strictly coarser than on $(X, \prec)$.

Corollary 3.134. For arbitrary well-founded $\prec_X, \prec_Y$, we have

(c) $(\lesssim_{X,Y}) = (\leq_Y \circ (\lesssim_{X,Y} \cap \gtrsim_{X,Y}))$, i.e., $x \lesssim_{X,Y} y \iff \exists y' \, (x \, (\lesssim \cap \gtrsim) \, y' \leq y)$.

Proof. Follows from Corollary 3.126(c) and Corollary 3.129. □

Corollary 3.135. $\lesssim$ is a global linear preorder between all well-founded relations: for well-founded $\prec_X, \prec_Y$, any $x \in X$ and $y \in Y$ are comparable.

Proof. By Proposition 3.124(a), WLOG $\eqsim_{X/\lesssim, Y/\lesssim}$ is an isomorphism between $X/\lesssim$ and an initial segment of $Y/\lesssim$. Then $[x] \eqsim [y']$ for some $y' \in Y$, and $[y'], [y]$ are comparable, hence so are x, y. □

As with the Mostowski collapse, we would now like to replace the well-ordered quotient $X/\lesssim$ with a global invariant for the equivalence relation $\lesssim \cap \gtrsim$.

Definition 3.136. Let $\prec \subseteq X^2$ be a well-founded relation, with transitive closure $<$. The **$\prec$-rank** of $x \in X$ is its $<$-Mostowski collapse

$$\rho(x) = \rho_\prec(x) := \mathord{\downarrow}_<(x) = \{\mathord{\downarrow}_<(y) \mid y < x\} = \{\rho(y) \mid y < x\};$$

by Corollary 3.114 and Exercise 3.15 as in the proof of Proposition 3.115, this is

$$\begin{aligned} &= \{\rho(y) \mid y \prec x \text{ or } \exists z \prec x \, (y < z)\} \\ &= \{\rho(y) \mid y \prec x\} \cup \textstyle\bigcup_{y \prec x} \{\rho(y') \mid y' < y\} \\ &= \{\rho(y) \mid y \prec x\} \cup \textstyle\bigcup_{y \prec x} \rho(y) \\ &= \textstyle\bigcup_{y \prec x} (\rho(y) \cup \{\rho(y)\}). \end{aligned}$$

The **rank** of $(X, \prec)$ is $\rho[X] = \mathord{\downarrow}_<[X]$.

Remark 3.137. As in Remark 3.95, this inductive definition is justified by Theorem 3.119.

Example 3.138. For $\prec$ = successor on $\mathbb{N}$, we compute

$$\begin{aligned} &\rho(0) = \varnothing, && \mathord{\downarrow}0 = \varnothing, \\ &\rho(1) = \rho(0) \cup \{\rho(0)\} = \{\rho(0)\} = \{\varnothing\}, && \mathord{\downarrow}1 = \{\varnothing\}, \\ &\rho(2) = \rho(1) \cup \{\rho(1)\} = \{\rho(0), \rho(1)\} = \{\varnothing, \{\varnothing\}\}, && \mathord{\downarrow}2 = \{\{\varnothing\}\}, \\ &\rho(3) = \rho(2) \cup \{\rho(2)\} = \{\rho(0), \rho(1), \rho(2)\} = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}, && \mathord{\downarrow}3 = \{\{\{\varnothing\}\}\}. \end{aligned}$$

(Of course, we will soon define $\mathbb{N}$ by declaring ρ here to be the identity; see Axiom 3.152.)

Corollary 3.139. For well-founded $\prec_X, \prec_Y$, we have

$$\begin{aligned} x \lesssim_{X,Y} y &\iff \rho(x) \Subset \rho(y), \\ x \, (\lesssim \cap \gtrsim) \, y &\iff \rho(x) = \rho(y). \end{aligned}$$

Here $\rho(x) \Subset \rho(y)$ means the reflexive closure of $\in$, i.e., either $\rho(x) \in \rho(y)$ or $\rho(x) = \rho(y)$. In fact, it is equivalent to $\subseteq$; see Proposition 3.149.

Proof. By Corollary 3.116 and Proposition 3.124,

$$x \lesssim y \iff \exists D \in Y/\lesssim ([x] \eqsim_{X/\lesssim, Y/\lesssim} D \leq [y]),$$

which after replacing the extensional quotients $X/\lesssim, Y/\lesssim$ with the isomorphic Mostowski collapses becomes precisely $\rho(x) \Subset \rho(y)$ (i.e., $\rho(x) \leq \rho(y)$ in the well-order $< = \in$ on $\rho[Y]$). □

3.G. **Ordinal numbers.**

Proposition 3.140 (cf. Proposition 3.105)**.** For a set α, the following are equivalent:

(i) α is transitive and $\in_\alpha \subseteq \alpha \times \alpha$ is a well-order.
(ii) α is transitive and $\in_\alpha$ is a partial well-order, i.e., transitive and well-founded.
(iii) α is transitive, each $\beta \in \alpha$ is transitive, and $\in_\alpha$ is well-founded (i.e., Foundation for α).
(iv) $\in_\alpha$ is a partial well-order and $\twoheaddownarrow_{\in_\alpha} = \mathrm{id}_\alpha$.
(v) $\in_\alpha$ is a partial well-order and $\alpha = \twoheaddownarrow_\in[\alpha]$.
(vi) $\in_\alpha$ is well-founded and $\rho_{\in_\alpha} = \mathrm{id}_\alpha$.
(vii) $\in_\alpha$ is well-founded and $\alpha = \rho_\in[\alpha]$.
(viii) $\alpha = \twoheaddownarrow_<[X]$ for some partial well-order $< \subseteq X^2$.
(ix) $\alpha = \twoheaddownarrow_< x$ for some partial well-order $< \subseteq X^2$ and $x \in X$.
(x) $\alpha = \rho_\prec[X]$ for some well-founded relation $\prec \subseteq X^2$.
(xi) $\alpha = \rho_\prec(x)$ for some well-founded relation $\prec \subseteq X^2$ and $x \in X$.

Proof. (i) $\iff$ (ii) by Proposition 3.122 (since $\in$ is always Extensional by the Axiom).
(ii) $\iff$ (iii): $\in_\alpha$ is transitive iff

$$\delta, \gamma \in \alpha \ \&\ \delta \in \gamma \in \beta \in \alpha \implies \delta \in \beta;$$

each $\beta \in \alpha$ is transitive iff this holds without assuming $\delta, \gamma \in \alpha$; but these follow from the second antecedent by transitivity of α.
(ii) $\iff$ (iv) as in Proposition 3.105.
(iv) $\implies$ (v) $\implies$ (viii) and (vi) $\implies$ (vii) $\implies$ (x) are obvious.
(iv) $\implies$ (vi), (v) $\implies$ (vii), (viii) $\implies$ (x), and (ix) $\implies$ (xi): By transitivity, $\twoheaddownarrow = \rho$.
(x) $\implies$ (viii) and (xi) $\implies$ (ix): By definition of rank, $\rho_\prec = \twoheaddownarrow_<$.
(viii) $\implies$ (ix): Add a new greatest element to X (as in Proposition 3.105).
(ix) $\implies$ (viii): Replace X with $\downarrow_< x$.
(vi) $\implies$ (i): Transitivity by Proposition 3.105; well-order because $(\alpha, \in) \cong (X/\approx, <)$. □

Definition 3.141. An **ordinal number** is a set obeying the above equivalent conditions.
The class of all ordinal numbers is denoted $\mathbb{ON}$ (also known as Ord or ∞[17]), and ordered via

$$\alpha < \beta \ :\iff\ \alpha \in \beta.$$

Proposition 3.142. $\mathbb{ON}$ is a transitive class, i.e., every element of an ordinal is an ordinal; and $\in$ is a well-order on the class $\mathbb{ON}$, where well-foundedness means:

(a) The **principle of transfinite induction**: if $B \subseteq \mathbb{ON}$ is a *subclass*, and every $\alpha \in \mathbb{ON}$ with $\alpha \subseteq B$ is in B, then $B = \mathbb{ON}$.
(b) Equivalently, every *class* $\varnothing \neq C \subseteq \mathbb{ON}$ has a $\in$-minimal element.
(c) In particular, this holds for nonempty sets C of ordinals.

Proof. Transitivity follows from e.g., Proposition 3.140(v).
$\in$ is a linear order by Corollary 3.139, since $\lesssim$ is by Corollary 3.135.
To prove (b): let $\alpha \in C$. If α is least in C, we're done. Otherwise, there is $\beta \in \alpha \cap C$, whence $\alpha \cap C \neq \varnothing$. Since $\alpha \cap C \subseteq \alpha$, it has a $\in$-least β, which is also $\in$-least in C since α is transitive. □

Corollary 3.143 (Burali-Forti paradox)**.** $\mathbb{ON}$ is a proper class.

Proof. Otherwise, it is an ordinal, whence $\mathbb{ON} \in \mathbb{ON}$, contradicting well-foundedness. □

Corollary 3.144. For a set of ordinals A, there is a **minimum excluded** ordinal $\operatorname{mex} A \notin A$. □

[17] because $\mathbb{ON}$ obeys the same properties as the ordinals, except for being a proper class, hence can be thought of as an "absolute infinity" bigger than all ordinals; see Corollary 3.143

Proposition 3.145. For a set of ordinals A, $\operatorname{mex} A = \{\alpha \in A \mid \alpha \subseteq A\}$.

Proof. If $\alpha \in \operatorname{mex} A$, i.e., $\alpha < \operatorname{mex} A$, then $\alpha \in A$ by definition of mex, and also every $\beta < \alpha$ is $< \operatorname{mex} A$, hence in A, which means $\alpha \subseteq A$.

Conversely, if $\alpha \in A$ and $\alpha \subseteq A$, i.e., every $\beta < \alpha$ is in A, then we cannot have $\operatorname{mex} A \leq \alpha$ since $\operatorname{mex} A \notin A$; thus $\alpha < \operatorname{mex} A$, i.e., $\alpha \in \operatorname{mex} A$. □

Corollary 3.146. If α is an ordinal, then $\operatorname{mex}(\alpha) = \alpha$. □

Example 3.147. There is a least ordinal

$$0 := \operatorname{mex} \varnothing = \varnothing,$$

and a next least

$$1 := \operatorname{mex}\{0\} = \{0\},$$

and a next least

$$2 := \operatorname{mex}\{0, 1\} = \{0, 1\},$$

etc. Note however that $\operatorname{mex}\{1\} = 0$.

Remark 3.148. For a set of ordinals $A \subseteq \mathbb{ON}$, to say that A is transitive is to say that A is $<$-downward-closed, in which case A is the set of all ordinals less than it.

Proposition 3.149.

(a) $\leq$ on $\mathbb{ON}$ is the same as $\subseteq$.

(b) A set of ordinals A has a least upper bound $\sup A = \bigcup A$, and a greatest upper bound $\inf A = \min A = \bigcap A$ if $A \neq \varnothing$.

(c) A set of ordinals A has a least *strict* upper bound $\sup^+ A := {\downarrow_{\leq}} A = A \cup \bigcup A = \sup_{\alpha \in A} \alpha^+$.

(d) An ordinal α has a **successor** $\alpha^+ := \sup^+\{\alpha\} = \alpha \cup \{\alpha\}$ (usually $\alpha + 1$; see Example 3.162).

Proof. (a) is true for any linear order: $a \leq b \iff {\downarrow_<} a \subseteq {\downarrow_<} b$. (If $a > b$, then $b \in {\downarrow_<} a \setminus {\downarrow_<} b$.)

(b) follows since $\bigcup$ and $\bigcap$ are sup and inf more generally for sets, and since the infimum must be achieved since A has a least element.

(c): To say $\sup^+ A$ is the least strict upper bound for A means its elements $< \sup^+ A$ must include every element of A but no other element $>$ every element of A, i.e., $\sup^+ A$ must consist of all elements $\leq$ some element of A, i.e., $\sup^+ A = {\downarrow_{\leq}} A$, i.e., $\sup^+ A$ consists of all elements $=$ or $<$ some element of A, i.e., $\sup^+ A = A \cup \bigcup A$.

(d) follows. Note also that to be a strict upper bound for every element of A means to be a non-strict upper bound for their successors; thus $\sup^+ A = \sup_{\alpha \in A} \alpha^+$. □

Remark 3.150. Definition 3.136 of rank of well-founded $\prec \subseteq X^2$ now says

$$\rho(x) = \sup^+_{y \prec x} \rho(y),$$
$$\rho[X] = \sup^+_{x \in X} \rho(x).$$

Definition 3.151. An ordinal α which is neither 0 nor a successor is called a **limit ordinal**. In other words, $0 < \alpha$, and for every $\beta < \alpha$, we have $\alpha \neq \beta^+$, whence $\beta^+ < \alpha$.

Axiom 3.152 (Infinity)**.** There exists a smallest limit ordinal, called $\mathbb{N}$ or ω.

Under the Axiom of Infinity, the ordinals look like:

$$0 < 1 < 2 < \cdots < \omega < \underbrace{\omega^+}_{=:\omega+1} < \underbrace{\omega^{++}}_{=:\omega+2} < \cdots < \sup^{(+)}\{\underbrace{\omega, \omega^+, \omega^{++}, \dots}_{=:\omega+\omega}\} < \cdots$$

We see that while ω is an "infinite" number, it is actually the smallest "infinity"; thus we use the more precise symbol ω, rather than ∞. (As noted above, when ∞ is used in a context involving ordinals, it usually denotes the "absolute infinity" $\mathbb{ON}$.)

Exercise 3.153. Suppose there exists a set X which contains $\varnothing$ and is closed under the operation $x \mapsto x \cup \{x\}$. Then by Knaster–Tarski, there is a smallest such X. Prove (without using Infinity or Foundation) that X is then transitive and $\in_X$ is transitive and well-founded, hence $X = \mathbb{N}$. Thus the Axiom of Infinity may also be stated as: there is a set containing $\varnothing$ and closed under $x \mapsto x \cup \{x\}$ (whence there is a smallest such set $\mathbb{N}$).

Definition 3.154. Zermelo–Fraenkel set theory ZF consists of the 7 axioms of $\mathsf{ZF}^- - \mathsf{Infinity}$ from Definition 2.26, plus the Axioms of Foundation 3.100 and Infinity 3.152.

ZF^- is the same but without Foundation.[18] The modern encoding of naturals (and more generally ordinals, i.e., well-orders up to bisimilarity/isomorphism) is called the *von Neumann encoding*.

By Exercise 3.153, we have the

Principle of ordinary induction. If $B \subseteq \mathbb{N}$ contains 0 and is closed under successor, then $B = \mathbb{N}$.

Proposition 3.155. Successor is injective on ordinals: if $\alpha^+ = \beta^+$, then $\alpha = \beta$.

Proof. This holds in general for linear orders (assuming successor exists). From $\alpha < \alpha^+ = \beta^+$, we get $\alpha \not> \beta$, whence $\alpha \leq \beta$. Similarly, $\beta \leq \alpha$. □

Exercise 3.156. Is $x \mapsto x \cup \{x\}$ injective on all sets? [The answer depends on Foundation.]

It follows from Proposition 3.155 that the (graph of the) successor function on $\mathbb{N}$ is indeed the graph we think it is: that each $0 \neq n \in \mathbb{N}$ is the successor of a unique $m \in \mathbb{N}$ (existence by the last condition in Knaster–Tarski; uniqueness by Proposition 3.155). Thus, the definition of $\mathbb{N}$ as the smallest closed under blah blah is induced by a well-founded relation; and so by Theorem 3.119,

Principle of ordinary inductive definition. Let $(Y_n)_{n\in\mathbb{N}}$ be a family of classes, and let

$$F_0 \in Y_0,$$
$$F_{n+1} : Y_n \to Y_{n+1}$$

for each n. Then there is a unique $f \in \prod_{n\in\mathbb{N}} Y_n$ such that

$$f(0) = F_0,$$
$$f(n+1) = F_{n+1}(f(n)).$$

Of course, by Proposition 3.142, we already have the principle of transfinite induction for all ordinals, of which *strong induction* for $\mathbb{N}$ is simply an initial segment. Similarly, we have the

Theorem 3.157 (principle of transfinite inductive definition)**.** Let $(Y_\alpha)_{\alpha\in\mathbb{ON}}$ be a family of classes,

$$\left(F_\alpha : \prod_{\beta\in\alpha} Y_\beta \to Y_\alpha\right)_{\alpha\in\mathbb{ON}}$$

be a (class) family of functions. Then there is a unique (class) $f \in \prod_{\alpha\in\mathbb{ON}} Y_\alpha$ such that

$$f(\alpha) = F_\alpha((f(\beta))_{\beta<\alpha}).$$

Proof. For each ordinal α, by Theorem 3.119, there is a unique $f_\alpha \in \prod_{\beta<\alpha} Y_\beta$ obeying this inductive definition. And for $\alpha \leq \beta$, f_α agrees with f_β on $\alpha \subseteq \beta$, since the latter also obeys this inductive definition. So the desired f is $\bigcup_{\alpha\in\mathbb{ON}} f_\alpha$. □

[18] Zermelo set theory Z^- is missing Foundation and Replacement, but includes Infinity; see (2.27). In fact, Zermelo originally introduced the "wrong" version of Infinity, where n is encoded as $\{\{\cdots\{\varnothing\}\cdots\}\}$; in other words, as the Mostowski collapse with respect to the successor graph, rather than the $<$ relation. It turns out that this version of Infinity is insufficient to prove the nowadays standard version, i.e., on some foundational level, *strong induction* really is stronger than *ordinary induction*!

3.H. **Ordinal arithmetic.**

Definition 3.158. The **sum** of two ordinals α, β is defined by induction on β as follows:

$$\begin{aligned}\alpha + \beta &:= \alpha \cup \{\alpha + \gamma \mid \gamma < \beta\} \\ &= \begin{cases} \alpha & \text{if } \beta = 0, \\ \sup^+_{\gamma<\beta}(\alpha+\gamma) & \text{if } \beta > 0, \end{cases} \\ &= \begin{cases} \alpha & \text{if } \beta = 0, \\ (\alpha+\gamma)^+ & \text{if } \beta = \gamma^+, \\ \sup_{\gamma<\beta}(\alpha+\gamma) & \text{if } \beta \text{ is a limit ordinal.} \end{cases}\end{aligned}$$

Exercise 3.159. How do these definitions fit into the formalism of Theorem 3.157?

Proposition 3.160. The three definitions above really are equivalent.

Proof. First, we show that the first two definitions are equivalent, by induction on β. Assume (IH) that for all $\gamma < \beta$, we have

$$\alpha \cup \{\alpha + \delta \mid \delta < \gamma\} = \begin{cases} \alpha & \text{if } \gamma = 0, \\ \sup^+_{\delta<\gamma}(\alpha+\delta) & \text{if } \gamma > 0. \end{cases}$$

If $\beta = 0$, then $\alpha \cup \{\alpha + \gamma \mid \gamma < \beta\} = \alpha$, as desired. Otherwise, we must show

$$\alpha \cup \{\alpha + \gamma \mid \gamma < \beta\} = \sup^+_{\gamma<\beta}(\alpha+\gamma)$$

where by the IH, the $\alpha+\gamma$ on both sides are the same. Everything in the LHS is either in $\alpha = \alpha+0$, hence in the RHS, or clearly in the RHS. Conversely, everything in the RHS is $\leq \alpha+\gamma$ for some $\gamma < \beta$, hence either equal to $\alpha+\gamma$ which is in the LHS, or in $\alpha+\gamma$, hence in $\alpha \cup \{\alpha+\delta \mid \delta < \gamma\} \subseteq$ LHS by the IH.

Next, note that by either the first or second definition,

Proposition 3.161. $+$ is strictly monotone in the second argument: $\gamma < \beta \implies \alpha+\gamma < \alpha+\beta$. □

Now we check that the second and third definitions are equivalent. If $\beta = \gamma^+$, then by monotonicity, the largest $\alpha+\delta$ among $\delta < \beta$ is $\alpha+\gamma$, hence the second definition reduces to $(\alpha+\gamma)^+$. And if β is a limit ordinal, then by strict monotonicity, the set of $\alpha+\delta$ for $\delta < \beta$ has no upper bound either, hence the $\sup^+$ reduces to a sup. □

Example 3.162. For any ordinal α, we have

$$\begin{aligned}\alpha + 0 &= \alpha, \\ \alpha + 1 &= (\alpha+0)^+ = \alpha^+.\end{aligned}$$

(So from now on, we will rarely write α^+.) The second clause of the above definition becomes

$$\alpha + (\gamma+1) = (\alpha+\gamma)+1.$$

Proposition 3.163. $+$ on ordinals is associative: $(\alpha+\beta)+\gamma = \alpha+(\beta+\gamma)$.

Proof. By induction on γ. If $\gamma = 0$, both sides simplify to $\alpha+\beta$. Otherwise,

$$(\alpha+\beta)+\gamma = \sup^+_{\delta<\gamma}((\alpha+\beta)+\delta) = \sup^+_{\delta<\gamma}(\alpha+(\beta+\delta)) = \alpha+(\beta+\gamma),$$

using the IH in the middle step, and in the last step that $\{\alpha+(\beta+\delta) \mid \delta < \gamma\}$ and $\{\alpha+\varepsilon \mid \varepsilon < \beta+\gamma\}$ have the same downward-closure by definition of $\beta+\gamma$. □

Exercise 3.164. Prove that $0+\alpha = \alpha$ for every ordinal α.

Example 3.165. We have $1+\omega = \sup^+\{1+0, 1+1, 1+2, \dots\} = \omega \neq \omega+1$. It follows by induction that $1+\alpha = \alpha \neq \alpha+1$ for any $\alpha \geq \omega$.

Proposition 3.166. $+$ on *naturals* is commutative: $m+n = n+m$ for all $m, n \in \mathbb{N}$.

Proof. First, we prove $1+n = n+1$ by induction on n. We have $1+0 = 1 = 0+1$. Assuming $1+n = n+1$, we have

$$\begin{aligned} 1+(n+1) &= (1+n)+1 && \text{by definition of } + \\ &= (n+1)+1 && \text{by IH.} \end{aligned}$$

We now prove it for arbitrary m by induction on n. We have

$$\begin{aligned} m+0 &= m && \text{by definition of } + \\ &= 0+m && \text{by Exercise 3.164.} \end{aligned}$$

Now suppose $m+n = n+m$. Then

$$\begin{aligned} m+(n+1) &= (m+n)+1 && \text{by definition of } + \\ &= (n+m)+1 && \text{by IH} \\ &= n+(m+1) && \text{by definition of } + \\ &= n+(1+m) && \text{by previous case} \\ &= (n+1)+m && \text{by associativity.} \end{aligned}$$

□

Exercise 3.167. Prove that $+$ is weakly monotone in the first argument: $\alpha \leq \beta \implies \alpha+\gamma \leq \beta \leq \gamma$.

Exercise 3.168. Prove that $\alpha \leq \beta$ iff $\alpha+\gamma = \beta$ for some γ, and in that case, γ is unique.

Exercise 3.169. Let β be an ordinal, and $(\alpha_\gamma)_{\gamma<\beta}$ be a family of ordinals. Define the **indexed sum** $\sum_{\gamma<\beta} \alpha_\gamma$ by induction on β as follows:

$$\begin{aligned} \textstyle\sum_{\gamma<0} \alpha_\gamma &:= 0, \\ \textstyle\sum_{\gamma<\beta+1} \alpha_\gamma &:= \textstyle\sum_{\gamma<\beta} \alpha_\gamma + \alpha_\beta, \\ \textstyle\sum_{\gamma<\beta} \alpha_\gamma &:= \sup_{\delta<\beta} \textstyle\sum_{\gamma<\delta} \alpha_\gamma \quad \text{for a limit ordinal } \beta. \end{aligned}$$

(a) How does this inductive definition fit into the formalism of Theorem 3.157?
(b) Verify that $\sum_{\gamma<1} \alpha_\gamma = \alpha_0$ and $\sum_{\gamma<2} \alpha_\gamma = \alpha_0 + \alpha_1$.
(c) Prove that $\sum_{\gamma<\beta} 1 = \beta$.

As a special case, define the **product** of ordinals α, β by

$$\alpha \cdot \beta := \textstyle\sum_{\gamma<\beta} \alpha.$$

(d) Conclude that $\alpha \cdot 1 = \alpha = 1 \cdot \alpha$.
(e) Prove that $\alpha \cdot 0 = 0 = 0 \cdot \alpha$.
(f) What are $\omega \cdot 2$, $2 \cdot \omega$?

We now give another perspective on ordinal sums and products. Let $(X, <_X)$ be a well-ordered set, and for each $x \in X$, let $(Y_x, <_{Y_X})$ be a well-ordered set. Recall from Definition 2.76

$$\textstyle\bigsqcup_{x\in X} Y_x := \{(x, y) \mid x \in X \ \&\ y \in Y_x\}.$$

The **lexicographical order** $<_{\text{lex}}$ on $\bigsqcup_{x\in X} Y_x$ is defined as in 3.24, and is a well-order as in 3.25.

(g) Prove that $\rho_{<_{\text{lex}}}[\bigsqcup_{x\in X} Y_x] = \sum_{\rho(x)<\rho[X]} \rho[Y_x]$. In particular, $\rho_{<_{\text{lex}}}[\bigsqcup_{\gamma<\beta} \alpha_\gamma] = \sum_{\gamma<\beta} \alpha_\gamma$.
(h) Prove the *indexed associative law*: for any ordinals γ, $(\beta_\delta)_{\delta<\gamma}$, and $(\alpha_{\delta,\varepsilon})_{\delta<\gamma, \varepsilon<\beta_\delta}$,

$$\textstyle\sum_{\delta<\gamma} \sum_{\varepsilon<\beta_\delta} \alpha_{\delta,\varepsilon} = \sum_{\rho_{<_{\text{lex}}}(\delta,\varepsilon)<\sum_{\delta<\gamma}\beta_\delta} \alpha_{\delta,\varepsilon}.$$

(i) Conclude that $\cdot$ on ordinals is associative and distributes over $\sum$ on one side [see (f)].

Exercise 3.170. Prove that $\cdot$ on *naturals* is commutative.

Exercise 3.171. What can you say about monotonicity of $\cdot$?

Exercise 3.172. Let β be an ordinal, and $(\alpha_\gamma)_{\gamma<\beta}$ be a family of ordinals. Define the **indexed product** $\prod_{\gamma<\beta}\alpha_\gamma$ inductively as follows:[19]

$$\begin{aligned}\textstyle\prod_{\gamma<0}\alpha_\gamma &:= 1,\\ \textstyle\prod_{\gamma<\beta+1}\alpha_\gamma &:= (\textstyle\prod_{\gamma<\beta}\alpha_\gamma)\cdot\alpha_\beta,\\ \textstyle\prod_{\gamma<\beta}\alpha_\gamma &:= \sup_{\delta<\beta}\textstyle\prod_{\gamma<\delta}\alpha_\gamma \quad \text{for a limit ordinal } \beta.\end{aligned}$$

In particular, for two ordinals α,β, define **ordinal exponentiation**

$$\alpha^\beta := \textstyle\prod_{\gamma<\beta}\alpha.$$

(a) What is 0^α? More generally, what is $\prod_{\gamma<\beta}\alpha_\gamma$ if some $\alpha_\gamma = 0$?
(b) What is 1^α?
(c) What is 2^ω? [See Footnote 19.]
(d) Prove that $(m\cdot n)^k = m^k\cdot n^k$ for *naturals* m,n,k. Give a counterexample for ordinals.

For a linearly ordered set $(X,<_X)$ and partially ordered sets $(Y_x,<_{Y_x})_{x\in X}$, the **lexicographical order** on $\prod_{x\in X}Y_x$ is given by

$$\vec{y}<_{\text{lex}}\vec{z} \;:\Longleftrightarrow\; \exists x\in X\,(y_x<z_x \;\&\; \forall x'<x\,(y_x=z_x)).$$

(e) Verify that this is a partial order.
(f) Verify that if $<_X$ is a well-order and each $<_{Y_x}$ is a linear order, then $<_{\text{lex}}$ is linear.
(g) Show that even if $<_X$ and each $<_{Y_x}$ are well-orders, $<_{\text{lex}}$ might not be.

Now suppose $>_X := <_X{}^{-1}$ is a well-order, and each $<_{Y_x}$ is a well-order, hence has a least element $0_x\in Y_x$. Let

$$\textstyle\bigoplus_{x\in X}Y_x := \big\{\vec{y}\in\prod_{x\in X}Y_x \;\big|\; \{x\in X\mid y_x\neq 0_x\} \text{ is finite}\big\}.$$

(*Finite* means there is a bijection with some $n\in\mathbb{N}$; see Definition 3.205.)

(h) Prove that $<_{\text{lex}}$ restricted to $\bigoplus_{x\in X}Y_x$ is a well-order.
(i) Prove that $\rho_{<_{\text{lex}}}[\bigoplus_{x\in X}Y_x] = \prod_{\rho_{>_X}(x)<\rho_{>_X}[X]}\rho[Y_x]$. In particular, $\rho_{<_{\text{lex}}}[\bigoplus_{\gamma<\beta}\alpha_\gamma] = \prod_{\gamma<\beta}\alpha_\gamma$ if every $\alpha_\gamma\neq 0$ (otherwise apply (a)), where $\bigoplus$ uses the order $\ni$ on β.
(j) Use this to prove that $\alpha^{\sum_{\delta<\gamma}\beta_\delta} = \prod_{\delta<\gamma}\alpha^{\beta_\delta}$.

We have built up the most fundamental number system $\mathbb{N}$ from the axioms of set theory. Developing other number systems, like $\mathbb{Z},\mathbb{Q}$, is really part of algebra; we give a brief sketch:

Exercise 3.173. A **commutative monoid** is a set N equipped with an associative and commutative binary operation $+$ with an identity element 0. It is **cancellative** if moreover,

$$x+y=x+z \implies y=z.$$

More generally, a submonoid $M\subseteq N$ is **cancellative** if this holds for all $x\in M$ and $y,z\in N$.

(a) Given a cancellative submonoid $M\subseteq N$, define an equivalence relation $\sim$ on $N\times M$ by

$$(a,b)\sim(c,d) \;:\Longleftrightarrow\; a+d=b+c.$$

Then $(N\times M)/{\sim}$ is an abelian group with an injective homomorphism $N\to(N\times M)/{\sim}$.
(b) Applied to $M=N:=\mathbb{N}$ with $+$ from Definition 3.158, this yields $\mathbb{Z}$.
(c) Applied to $N:=\mathbb{Z}$, $M:=\mathbb{N}\setminus\{0\}$, and $+:=\cdot$, this yields $\mathbb{Q}$.
(d) If moreover N is a **rig**, meaning equipped an associative and unital operation $\cdot$ distributing over $+$, then $(N\times M)/{\sim}$ becomes a ring under $[(a,b)]\cdot[(c,d)] := [(ac+bd,ad+bc)]$.

[19] Warning: this is distinct from cardinal product; see Remark 4.32. Unlike the indexed sum, the indexed product of ordinals doesn't even have the same cardinality as the cardinal product.

3.I. **The revenge of Knaster–Tarski.** Recall that the proof of Knaster–Tarski given in Theorem 3.6 was "top-down" or *impredicative* (Remark 3.13). Using transfinite induction, we now give a "bottom-up" proof, that also has the benefit of generalizing to proper classes (to a certain extent).

Definition 3.174. For a class X, the **powerclass** $\mathcal{P}(X) = \{A \mid A \subseteq X\}$ is defined as before (Example 2.6). Note that this is now the *class* of all sub*sets* of X, since the elements of a comprehension must be sets. In particular, if X is a proper class, $\mathcal{P}(X)$ has no greatest element.

Definition 3.175. Let X be a class. A **monotone set operator** $T : \mathcal{P}(X) \to \mathcal{P}(X)$ means the same thing as in Definition 3.1, i.e., a monotone *class* function mapping each sub*set* to another.

Given such T, if we instead have a sub*class* $A \subseteq X$, we define

$$\begin{aligned} T(A) &:= \bigcup\{T(B) \mid B \subseteq A\} \\ &= \{x \mid \exists B \subseteq A\, (x \in T(B))\}. \end{aligned}$$

Again, here B ranges over all sub*sets*. Note that if A happens to be a subset, then there is a largest such $B \subseteq A$, namely A; hence this agrees with the original value of T on A (using monotonicity).

We say a subclass $A \subseteq X$ is **T-closed** if $T(A) \subseteq A$, i.e., $T(B) \subseteq A$ for every sub*set* $B \subseteq A$.

Theorem 3.176 (Knaster–Tarski II)**.** Let X be a class, $T : \mathcal{P}(X) \to \mathcal{P}(X)$ be a monotone set operator, $A \subseteq X$ be a sub*set*. Define sets $A_\alpha \subseteq X$ for each $\alpha \in \mathbb{ON}$ by induction as follows:

$$\begin{aligned} A_0 &:= A, \\ A_{\alpha+1} &:= A_\alpha \cup T(A_\alpha), \\ A_\alpha &:= \textstyle\bigcup_{\beta<\alpha} A_\beta \quad \text{for a limit ordinal } \alpha. \end{aligned}$$

This is equivalent to

$$\begin{aligned} A_\alpha &:= \textstyle\bigcup_{\beta<\alpha}(A_\beta \cup T(A_\beta)) \quad \text{for } \alpha > 0, \\ A_\alpha &:= A \cup \textstyle\bigcup_{\beta<\alpha} T(A_\beta) \quad \text{for all } \alpha. \end{aligned}$$

Then $(A_\alpha)_\alpha$ is a monotone transfinite sequence, i.e., $\beta \le \alpha \implies A_\beta \subseteq A_\alpha$; and

$$\overline{T}(A) := \textstyle\bigcup_{\alpha\in\mathbb{ON}} A_\alpha$$

is the smallest T-closed subclass of X containing A. Moreover, if $A \subseteq T(A)$, then we have

$$\begin{aligned} A_{\alpha+1} &:= T(A_\alpha), \\ A_\alpha &:= \textstyle\bigcup_{\beta<\alpha} T(A_\beta) \quad \text{for } \alpha > 0, \end{aligned}$$

hence $T(\overline{T}(A)) = \overline{T}(A)$. In particular, this holds for $A = \varnothing$. (See the picture (3.14).)

Proof. First, we assume that $A \subseteq T(A)$. We take $A_0 := A$ and the last equation as the definition of A_α for $\alpha > 0$. We then have $A_\alpha \subseteq T(A_\alpha)$ for all α: for $\alpha > 0$, assuming $A_\beta \subseteq T(A_\beta) \subseteq A_\alpha$ for all $\beta < \alpha$, we have $T(A_\beta) \subseteq T(A_\alpha)$ for all $\beta < \alpha$, whence $A_\alpha = \bigcup_{\beta<\alpha} T(A_\beta) \subseteq T(A_\alpha)$. Then $\beta < \alpha \implies A_\beta \subseteq T(A_\beta) \subseteq A_\alpha$, i.e., the sequence is monotone. It follows that all of the definitions of A_α are equivalent, except for $A_\alpha = \bigcup_{\beta<\alpha} A_\beta$ for limit α; this one is clearly $\subseteq$ the last equation, while for $\beta < \alpha$, then $\beta + 1 < \alpha$, whence $T(A_\beta) = A_{\beta+1} \subseteq \bigcup_{\beta<\alpha} A_\beta$. Thus the definitions agree.

We now verify that $\overline{T}(A) \subseteq X$ is the smallest T-closed subclass containing A. If $B \subseteq X$ is any T-closed subclass containing A, then we prove $\overline{T}(A) = \bigcup_\alpha A_\alpha \subseteq B$, i.e., $A_\alpha \subseteq B$ for all α, by induction on α: we have $A_0 = A \subseteq B$, and for $\alpha > 0$, assuming $A_\beta \subseteq B$ for all $\beta < \alpha$, then $T(A_\beta) \subseteq T(B) \subseteq B$ for all $\beta < \alpha$, whence $A_\alpha = \bigcup_{\beta<\alpha} T(A_\beta) \subseteq B$. We have $A = A_0 \subseteq \overline{T}(A)$. To show $\overline{T}(A)$ is T-closed, let $B \subseteq \overline{T}(A)$ be a sub*set*, and for each $x \in B$, let α_x be least such that $x \in A_{\alpha_x}$; then letting $\alpha := \sup_{x\in B} \alpha_x$, we have $B \subseteq A_\alpha$, whence $T(B) \subseteq T(A_\alpha) = A_{\alpha+1} \subseteq \overline{T}(A)$.

This concludes the proof assuming $A \subseteq T(A)$ for all $A \in \mathcal{P}(X)$. To deduce the general case, apply the special case to $T'(A) := A \cup T(A)$, or to $T_A(B) := A \cup T(B)$ from Exercise 3.15. □

In the case where $A \subseteq T(A)$, so that $A_{\alpha+1} = T(A_\alpha)$, it is convenient to think of A_α as the "αth iterate of T of A":

$$T^\alpha(A) := \begin{cases} A & \text{if } \alpha = 0, \\ \bigcup_{\beta<\alpha} T(T^\beta(A)) & \text{if } \alpha > 0. \end{cases}$$

(It is literally $(T \circ \cdots \circ T)(A)$ when $\alpha \in \mathbb{N}$.) Then thinking of $\mathbb{ON}$ as "∞", we write

$$T^\infty(A) := \overline{T}(A) = \bigcup_{\alpha<\infty} T^\alpha(A).$$

In particular, we may always write these for $A = \varnothing$.

Definition 3.177. For a monotone set operator $T : \mathcal{P}(X) \to \mathcal{P}(X)$ and $x \in \overline{T}(\varnothing) = T^\infty(\varnothing)$, the **$T$-rank** of x is

$$\rho_T(x) := \min\{\alpha \in \mathbb{ON} \mid x \in T^{\alpha+1}(\varnothing)\}.$$

(Note that the least β with $x \in T^\beta(\varnothing)$ must be a successor, since $T^\beta(\varnothing) = \bigcup_{\alpha<\beta} T^\alpha(\varnothing)$ for limit β.)

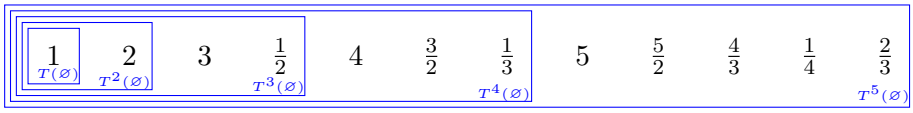
Exercise 3.178. For a well-founded $\prec \subseteq X^2$, we have $\rho_\prec = \rho_{T_\prec}$.

(In particular, the sequence $T^0(\varnothing) \subseteq T^1(\varnothing) \subseteq \cdots$ may take arbitrarily long to stabilize.)

Example 3.179. Let $\mathbb{Q}^+$ be the positive rationals, and let

$$\begin{aligned} T : \mathcal{P}(\mathbb{Q}^+) &\longrightarrow \mathcal{P}(\mathbb{Q}^+) \\ A &\longmapsto \{1\} \cup \{q+1 \mid q \in A\} \cup \{q^{-1} \mid q \in A\}. \end{aligned}$$

The first few iterations look like:



This T is inductive, so $\mathbb{Q}^+ = T^\infty(\varnothing)$; in fact, $T^\omega(\varnothing) = \bigcup_{n<\omega} T^n(\varnothing)$ is already $T^\infty(\varnothing)$, since anything derivable from it is already derivable from $T^n(\varnothing)$ for some finite n, hence is in $T^{n+1}(\varnothing)$.

This is a general piece of extra information that the "bottom-up" proof of Knaster–Tarski yields:

Proposition 3.180. Suppose a monotone set operator $T : \mathcal{P}(X) \to \mathcal{P}(X)$ is **finitary**, meaning that whenever $x \in T(A)$, then $x \in T(B)$ for some finite $B \subseteq A$.[20] Then the transfinite sequence $(A_\alpha)_{\alpha\in\mathbb{ON}}$ from Theorem 3.176 stabilizes at A_ω, i.e., $A_\alpha = A_\omega$ for all $\alpha \geq \omega$. Thus $\overline{T}(A) = A_\omega$. Moreover, $\overline{T} : \mathcal{P}(X) \to \mathcal{P}(X)$ is also finitary; and if T maps finite sets to countable sets, then $\overline{T}$ preserves countable sets.

Proof. If $x \in T(A_\omega)$, then there is a finite $B \subseteq A_\omega = \bigcup_{n<\omega} A_n$ such that $x \in T(B)$, whence $B \subseteq A_n$ for some n, whence $x \in T(B) \subseteq T(A_n) \subseteq A_{n+1} \subseteq A_\omega$; thus A_ω is T-closed and contains $A_0 = A$, and is contained in $\overline{T}(A)$ by definition, hence is equal to $\overline{T}(A)$. This proves the first claim.

To show that $\overline{T}$ is finitary: if $T_i : \mathcal{P}(X) \to \mathcal{P}(X)$ are an arbitrary family of finitary monotone set operators, then it is easily seen that $A \mapsto \bigcup_i T_i(A)$ is finitary as well. Also, if $S, T : \mathcal{P}(X) \to \mathcal{P}(X)$ are both finitary monotone, then so is $S \circ T$, since if $x \in S(T(A))$, then $x \in S(B)$ for a finite $B \subseteq T(A)$, and each $y \in B$ is in $T(C_y)$ for a finite $C_y \subseteq A$, whence letting $C := \bigcup_{y\in B} C_y$, we have $B \subseteq T(C)$, whence $x \in S(B) \subseteq S(T(C))$. It follows by induction that for each α, $A \mapsto A_\alpha = A \cup \bigcup_{\beta<\alpha} T(A_\beta)$ is finitary; in particular, $\overline{T}(A) = A_\omega$ is finitary.

Finally, suppose T maps finite sets to countable sets. Then T also maps countable sets to countable sets, since if $A = \{x_0, x_1, \dots\}$ is countable, then $T(A) = \bigcup_{n<\omega} T(\{x_0, x_1, \dots, x_{n-1}\})$ since T is finitary. By induction, we then easily have that for any countable ordinal α, if A is countable, then so is $A_\alpha = A \cup \bigcup_{\beta<\alpha} T(A_\beta)$; in particular, $\overline{T}(A) = A_\omega$ is countable. □

[20] Other synonymous terminology include **of finite character**, **Scott-continuous**.

Corollary 3.181. For a finitary T on a class X, T-closure preserves sets. □

Remark 3.182. Analogous bounds hold for cardinalities higher than countable; see Corollary 4.51 and Exercises 4.71 and 4.93. (Indeed, the definition of *monotone set operator* can be regarded as saying that T is "set-ary": whenever $x \in T(A)$ for a class A, then $x \in T(B)$ for a sub*set* $B \subseteq A$.)

Example 3.183. For an algebraic structure X as in Example 3.4 equipped with *finitary* operations $f_i : X^{n_i} \to X$, where $n_i \in \mathbb{N}$, the T which closes under the operations is finitary. (Example 3.179 is a special case, where we only have nullary and unary operations.)

If there are moreover only countably many such operations (i.e., the index set I is countable), then T maps finite A to a countable union of finite $T(A) = \bigcup_i f_i[A^{n_i}]$, whence we get that a countable subset $A \subseteq X$ generates a countable subalgebra $\overline{T}(A) \subseteq X$.

For example, the subgroup or subring of $\mathbb{R}$ generated by a countable subset is countable, etc.

Example 3.184. In contrast, consider $\mathcal{P}(\mathbb{R})$ equipped with the *countable* Boolean operations (union, intersection, complement). Let $\mathcal{A} \subseteq \mathcal{P}(\mathbb{R})$ denote all countably many open intervals (a, b) with rational endpoints $a, b \in \mathbb{Q}$. Note that we may close $\mathcal{A}$ under countable Boolean operations via

$$\begin{aligned} T : \mathcal{P}(\mathbb{R}) &\longrightarrow \mathcal{P}(\mathbb{R}) \\ \mathcal{A} &\longmapsto \{\mathbb{R} \setminus \textstyle\bigcup_{i\in I} A_i \mid I \text{ countable}, (A_i)_{i\in I} \in \mathcal{A}^I\}. \end{aligned}$$

Applying $T(\mathcal{A})$ once already yields all closed sets, of which there are uncountably many. The transfinite sequence $\mathcal{A}_0 \subseteq \mathcal{A}_1 \subseteq \cdots$ looks like:

- $\mathcal{A}_1$: all closed sets
- $\mathcal{A}_2$: all G_δ = countable intersection of open sets, e.g., $\mathbb{R} \setminus \mathbb{Q}$
- $\mathcal{A}_3$: all countable intersections of F_σ sets, e.g., all **normal** numbers $x \in \mathbb{R}$ (meaning every finite block of n digits occurs in x with average density 10^{-n}).

It turns out that this sequence does not stabilize at any countable ordinal stage!

Proof sketch. One can show by induction that for each countable ordinal α, there is a set $U_\alpha \subseteq \mathbb{R}^2$ such that the "vertical cross-sections" $(U_\alpha)_x = \{y \in \mathbb{R} \mid (x, y) \in U_\alpha\}$ for each $x \in \mathbb{R}$ are precisely all of the sets in $\mathcal{A}_\alpha$, and the diagonal $D_\alpha = \{x \in \mathbb{R} \mid (x, x) \in U_\alpha\}$ is *also* in $\mathcal{A}_\alpha$; essentially, one defines $(U_\alpha)_x$ to be the complement of the intersections of certain $(U_\beta)_y$'s for $\beta < \alpha$ as specified by the digits of x. But then, Cantor's diagonalization argument (Theorem 2.9) shows that $\mathbb{R} \setminus D^\alpha \notin \mathcal{A}_\alpha$. □

Remark 3.185. This sequence is called the **Borel hierarchy** $\mathcal{A}_\alpha = \mathbf{\Pi}^0_\alpha$ in descriptive set theory.

There is an analogous hierarchy of maps $\mathbb{R} \to \mathbb{R}$, obtained by starting with the continuous maps and then repeatedly closing pointwise limits of sequences, called the **Baire hierarchy**, which also takes uncountably many steps to stabilize at the class of **Borel-measurable** maps $\mathbb{R} \to \mathbb{R}$.

Exercise 3.186. Show that for a monotone set operator $T : \mathcal{P}(X) \to \mathcal{P}(X)$ on a class X, the T-interior $T^\circ(A)$ (cf. Exercise 3.68) of every subclass $A \subseteq X$ exists, and is a set if A is.

Exercise 3.187. Let

$$\begin{aligned} T : \mathcal{P}(\mathbb{ON}) &\longrightarrow \mathcal{P}(\mathbb{ON}) \\ A &\longmapsto \operatorname{mex}(A)^+. \end{aligned}$$

(a) Prove that $\overline{T}(A) = \mathbb{ON}$ for any subset $A \subseteq \mathbb{ON}$, which is not very interesting.

(b) For $\alpha \in \mathbb{ON}$, consider the transfinite sequence $(\alpha_\beta)_{\beta\in\mathbb{ON}}$ in Theorem 3.176 used to build $\overline{T}(\alpha)$. Verify that the various definitions of this sequence in Theorem 3.176 correspond to the various definitions of $\alpha + \beta$ in Definition 3.158. Using this, deduce Proposition 3.160.

(c) In a similar manner, deduce that $\cdot$ from Exercise 3.169 may also be defined via

$$\alpha \cdot \beta = \sup_{\gamma<\beta}(\alpha \cdot \gamma + \alpha).$$

[Hint: instead of $\overline{T}(\alpha)$, take $\overline{T_\alpha}(\varnothing)$ for a suitable T_α depending on α.]

3.J. **Transitive closure, $\in$-induction, and the cumulative hierarchy.** The axioms of set theory yield two basic monotone set operators on the universe V, namely $\bigcup$ and $\mathcal{P}$. Note that[21]

$$\bigcup A \subseteq B \iff A \subseteq \mathcal{P}(B) \tag{3.188}$$

for any classes $A, B \subseteq V$. Thus in particular, A is $\bigcup$-closed iff it is $\mathcal{P}$-open, iff it is transitive.

Definition 3.189. The **transitive closure** of a class A is the smallest transitive class $\overline{\bigcup} A \supseteq A$. Since $\bigcup$ is clearly a finitary (indeed unary) monotone set operator, by Proposition 3.180,

$$\overline{\bigcup} A = A \cup \bigcup A \cup \bigcup\bigcup A \cup \cdots = \bigcup_{n\in\mathbb{N}} \bigcup^n A;$$

in particular, the transitive closure of a set is still a set.[22]

Example 3.190. $\overline{\bigcup}\{\{\varnothing\}\} = \{\{\varnothing\}\} \cup \{\varnothing\} \cup \varnothing = \{\{\varnothing\}, \varnothing\} = 2$.

Corollary 3.191. For every set x, there is a set X containing x such that $x = {\downarrow_{\in_X}} x$.

Proof. Let $X = \overline{\bigcup}\{x\} = \{x\} \cup x \cup \bigcup x \cup \bigcup\bigcup x \cup \cdots$; then for every $y \in X$, by transitivity,

$${\downarrow_{\in_X}} y = \{z \in X \mid z \in y\} = \{z \mid z \in y\} = y. \qquad \square$$

Corollary 3.192 (Axiom (Schema) of ($\in$-)Induction)**.** Assume ZF, and let $\phi(x)$ be a property. If

- for every set x, if every $y \in x$ satisfies $\phi(y)$, then $\phi(x)$,

then for every set x, $\phi(x)$. In other words, the global $\in$ relation on V is well-founded.

Proof. To show $\phi(x)$, by Foundation, we may do $\in_X$-induction on $X = \overline{\bigcup}\{x\}$. $\square$

Remark 3.193. Conversely, clearly well-foundedness of the global $\in$ implies well-foundedness of $\in_X$ on each set X, i.e., Induction implies Foundation.[23] This is analogous to the passage between well-foundedness of each ordinal α versus well-foundedness of the entire class of ordinals $\mathbb{ON}$ in Proposition 3.142.

Exercise 3.194. Every class A also has a **transitive interior** $\mathcal{P}^\circ(A)$ by Exercise 3.186. Show that

$$\mathcal{P}^\circ(A) = A \cap \mathcal{P}(A) \cap \mathcal{P}(\mathcal{P}(A)) \cap \cdots.$$

This covers two possible combinations of closure/interior and $\bigcup/\mathcal{P}$, that are related via (3.188). What about the other two combinations? One of them is again related to Foundation: note that

$$\mathcal{P}(A) = \{x \mid \forall y \in x\, (y \in A)\} = T_\in(A) \tag{3.195}$$

is the monotone set operator induced (as in Definition 3.32) by the relation $\in \subseteq V^2$.

Definition 3.196. The **von Neumann cumulative hierarchy** is the transfinite sequence used to build $\overline{\mathcal{P}}(\varnothing)$ as in the Knaster–Tarski Theorem 3.176:

$$\begin{aligned}
V_0 &:= \mathcal{P}^0(\varnothing) = \varnothing,\\
V_1 &:= \mathcal{P}^1(\varnothing) = \{\varnothing\},\\
V_2 &:= \mathcal{P}^2(\varnothing) = \{\varnothing, \{\varnothing\}\},\\
V_3 &:= \mathcal{P}^3(\varnothing) = \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\varnothing, \{\varnothing\}\}\},\\
V_\alpha &:= \mathcal{P}^\alpha(\varnothing) = \textstyle\bigcup_{\beta<\alpha} \mathcal{P}(V_\beta).
\end{aligned}$$

Thus, $V_\infty := \overline{\mathcal{P}}(\varnothing)$ is the well-founded part of the universe. The **rank** $\rho(x)$ of $x \in V_\infty$ is its $\in$-rank

$$\rho(x) := \rho_\in(x) = \min\{\alpha \in \mathbb{ON} \mid x \in V_{\alpha+1} = \mathcal{P}(V_\alpha)\}.$$

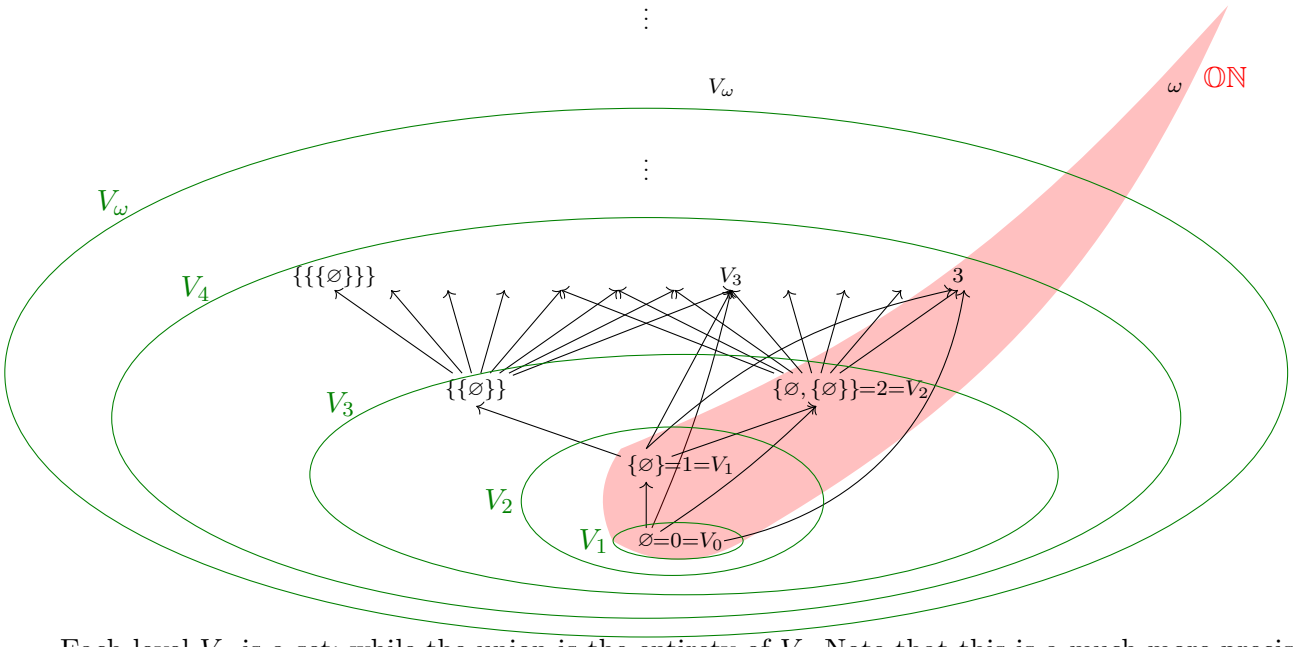
[21] In other words, $\bigcup$ and $\mathcal{P}$ form a (monotone) Galois adjunction $\mathcal{P}(V) \rightleftarrows \mathcal{P}(V)$.

[22] It turns out that this fact cannot be proved without the Axiom of Infinity!

[23] Once again, in the absence of Infinity, Induction is strictly stronger than Foundation.

Corollary 3.197. Assuming only $\mathsf{ZF}^- - \mathsf{Infinity}$, Induction (hence Foundation, assuming Infinity) is equivalent to $V = V_\infty$, i.e., every set x is in V_α for some ordinal α. □

Thus, the universe under Foundation (or Induction, in the absence of Infinity) looks like:



Each level V_α is a set; while the union is the entirety of V. Note that this is a much more precise version of the picture (2.12): the "boundary" of the universe is the upper fringe; a class $A \subseteq V$ is proper iff it keeps going up, i.e., is not contained in any V_α. For a set A, the least α such that $A \subseteq V_\alpha$, i.e., $A \in V_{\alpha+1}$, is its rank $\rho(A)$. The ordinals $\mathbb{ON}$ form a linearly ordered "spine" that contains exactly one representative of each rank α (namely α).

Corollary 3.198. Assume Foundation (or Induction, in the absence of Infinity). Then any other class $A \subseteq V$ can also be written as a transfinite increasing union of sets, namely $A = \bigcup_{\alpha\in\mathbb{ON}}(A \cap V_\alpha)$. □

An important application is a way of building "quotients" by proper class-sized equivalence relations. Given an equivalence relation $\sim \subseteq X^2$, the point of the quotient set construction is to represent each $x \in X$ by some "invariant" such that $\sim$ between x's becomes equality between invariants. The usual equivalence class $[x]$ takes all elements equivalent to x; if $\sim$ (hence X) is a proper class, then $[x]$ may also be, hence need not exist in the universe even though x does. But we may instead take a sub*set* of $[x]$ as the "invariant". For example, this gives one possible representation of "cardinal numbers" within the universe; see Definition 4.3.

Corollary 3.199 (Scott's trick)**.** Assume Foundation. Let X be a class, $\sim \subseteq X^2$ be an equivalence relation (also a class). Then there is a (class) function $\pi : X \to V$ such that $\pi(x) = \pi(y) \iff x \sim y$.

Proof. Let $\alpha(x) := \min\{\alpha \in \mathbb{ON} \mid [x] \cap V_\alpha \neq \varnothing\}$, which is always defined since $x \in V_\alpha$ for some α by Foundation, and $\pi(x) := [x] \cap V_{\alpha(x)}$. If $x \sim y$, then $[x] = [y]$, whence $\alpha(x) = \alpha(y)$ and $\pi(x) = \pi(y)$. Conversely, if $\pi(x) = \pi(y)$, then there is some $z \in [x] \cap V_{\alpha(x)} = \pi(x)$ by definition of $\alpha(x)$, whence also $z \in \pi(y) \subseteq [y]$, whence $x \sim z \sim y \implies x \sim y$. □

Exercise 3.200. Show (assuming ZF) that V_ω consists precisely of the **hereditarily finite sets**, i.e., which are finite, all of whose elements are finite, etc. (First formalize what this "etc." means.)

Exercise 3.201. Show (assuming ZF) that if A is a $\bigcup$-open set, then $\rho(A)$ is either 0 or a limit ordinal. (I don't know of any particular conceptual significance of such sets, unfortunately.)

3.K. **The axiom of choice.** Given a well-ordered set, we may prove statements and construct things for each element one by one. (Whereas for a general well-founded relation, we sort of have to handle incomparable elements simultaneously, since they are not allowed to depend on each other.) It is thus of interest to know: which sets can be well-ordered?

Proposition 3.202. For a set X, the following are equivalent:

(i) There exists a well-order $<$ on X (we say X is **well-orderable**).
(ii) There exists a bijection between X and an ordinal.
(iii) There exists an injection from X into a well-ordered set.
(iv) There exists a surjection from a well-ordered set onto X.
(v) There exists a **choice function** $c \in \prod_{A \in \mathcal{P}(X) \setminus \{\varnothing\}} A$, i.e., $c : \mathcal{P}(X) \setminus \{\varnothing\} \to X$ such that $c(A) \in A$ for each $\varnothing \neq A \subseteq X$.
(vi) For any set I and family of nonempty subsets $(A_i)_{i \in I} \in (\mathcal{P}(X) \setminus \{\varnothing\})^I$, $\prod_{i \in I} A_i \neq \varnothing$.
(vii) For any set I and relation $R \subseteq I \times X$ with $\mathrm{dom}(R) = I$, there is a function $R \supseteq f : I \to X$.

Proof. (i) $\implies$ (ii): The rank function $\rho_< : X \cong \rho_<[X]$ is a bijection.
(ii) $\implies$ (iv) is obvious.
(iv) $\implies$ (iii): Let $(Y, <)$ be well-ordered, $f : Y \twoheadrightarrow X$; then $g : X \hookrightarrow Y$ where $g(x) := \min f^{-1}(x)$.
(iii) $\implies$ (i): Let $(Y, <)$ be well-ordered, $f : X \hookrightarrow Y$; then $x < x' :\iff f(x) < f(x')$ well-orders X.
(v) $\implies$ (vi): $(c(A_i))_{i \in I} \in \prod_{i \in I} A_i$.
(vi) $\iff$ (vii) follows from the canonical bijection $\mathcal{P}(I \times X) \cong \mathcal{P}(X)^I$ (Exercise 2.82).
(vii) $\implies$ (v): Take $R := \ni \subseteq (\mathcal{P}(X) \setminus \{\varnothing\}) \times X$.
(i) $\implies$ (v): $c(A) := \min A$.
(v) $\implies$ (ii): Define $A_\alpha \subseteq X$, which is either empty or a singleton, for each $\alpha \in \mathbb{ON}$ inductively:

$$A_\alpha := \begin{cases} \varnothing & \text{if } \bigcup_{\beta<\alpha} A_\beta = X, \\ \{c(X \setminus \bigcup_{\beta<\alpha} A_\beta)\} & \text{else.} \end{cases}$$

Note that if $A_\alpha = \varnothing$, then clearly $A_\beta = \varnothing$ for all $\beta > \alpha$. Also, if $A_\alpha, A_\beta \neq \varnothing$ and $\alpha \neq \beta$, WLOG with $\beta < \alpha$, then (the unique elements of) A_α, A_β differ by definition of A_α. We thus have an injection from an initial segment of $\mathbb{ON}$, namely all those α such that $A_\alpha \neq \varnothing$, mapping such α to the unique element of $A_\alpha \subseteq X$. Since X is a set, the initial segment of those α's must also form a set, hence an ordinal $\gamma \subseteq \mathbb{ON}$, such that $A_\gamma = \varnothing$ since $\gamma \notin \gamma$; thus $\alpha \mapsto$ unique element of A_α is a bijection $\gamma \cong X$. □

Axiom 3.203 (Choice (AC))**.** Every set is well-orderable, i.e., the equivalent conditions above hold. (Conditions (i) to (iv) are known as the **well-ordering theorem**.)

Definition 3.204. Zermelo–Fraenkel set theory with **Choice** ZFC consists of the axioms of ZF (Definition 3.154) together with the Axiom of Choice. (See the diagram (2.27).)

The Axiom of Choice is unique among the axioms of ZFC in asserting the existence of a mathematical object, namely a choice function or a well-order, which obeys certain properties that by no means uniquely characterize it. By contrast, most of the other axioms (2.27) are special cases of unrestricted Comprehension, which assert the existence of a set which is necessarily unique by Extensionality (while Foundation asserts that certain kinds of sets *don't* exist). For this reason, Choice is often regarded as a "non-constructive" axiom; see Theorem 3.221.

Nonetheless, the Axiom of Choice is extremely useful, to the point that one often uses it without thinking, and doing math without it can feel quite bizarre, as the following basic applications illustrate:

Definition 3.205. A set X is **finite** if there exists a bijection between X and a natural.

Proposition 3.206. If a set X is infinite (i.e., not finite), then there is an injection $f : \mathbb{N} \hookrightarrow X$.

Proof. Choose inductively $f(n) \in X \setminus f[n]$; this is always possible, or else we would have $f : n \cong X$.

More precisely, we first fix a choice function $c \in \prod_{A \in \mathcal{P}(X)\setminus\{\varnothing\}} A$, and then define $A_n \subseteq X \setminus \bigcup_{m<n} A_m$ which is either empty or a singleton $\{f(n)\}$ inductively for each $n \in \mathbb{N}$ as in Proposition 3.202. Having done so, we may show that $A_n \neq \varnothing$ for all n, or else for the least n such that $A_n = \varnothing$, we would have a bijection $f : n \cong X$ taking each $m < n$ to the unique element of A_m.

Or more concisely, we've already done the work in Proposition 3.202 of showing that there exists a bijection $f : \alpha \cong X$ from an *ordinal*; now by assumption, α is not a natural, hence $\omega \leq \alpha$, and so the restriction of f to ω is the desired injection. □

Exercise 3.207. Show that if $A \subseteq \mathbb{R}$ has no upper bound (i.e., no $b \in \mathbb{R}$ such that $a \leq b$ for all $a \in A$), then there is a sequence $\mathbb{N} \to A$ converging to ∞. Be explicit about uses of Choice.

The preceding two applications of Choice both follow from the following weakening:

Exercise 3.208 (Countable Dependent Choice (DC))**.** Show (over ZF) that the following statements are equivalent:

(i) For every set $X \neq \varnothing$ and relation $R \subseteq X^2$ with $\mathrm{dom}(R) = X$, there exists a sequence $f : \mathbb{N} \to X$ such that $f(n)\ R\ f(n+1)$ for all $n \in \mathbb{N}$.

(ii) For every sequences of sets $(X_n)_{n\in\mathbb{N}}$ with $X_0 \neq \varnothing$ and relations $(R_n \subseteq X_n \times X_{n+1})_{n\in\mathbb{N}}$ with $\mathrm{dom}(R_n) = X_n$, there exists a sequence $f \in \prod_{n\in\mathbb{N}} X_n$ such that $f(n)\ R_n\ f(n+1)$ for all n.

Show that these statements are implied by the full Axiom of Choice, and explain how the above two results follow from ZF + DC.

Exercise 3.209. Show using DC that for a function $f : \mathbb{R} \to \mathbb{R}$, the following are equivalent:

(i) For every convergent sequence $(x_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$, $\lim_{n\to\infty} f(x_n) = f(\lim_{n\to\infty} x_n)$.

(ii) For every $\varepsilon > 0$ and $x \in \mathbb{R}$, there exists $\delta > 0$ such that for every $y \in \mathbb{R}$ with $|x - y| < \delta$, we have $|f(x) - f(y)| < \varepsilon$.

Exercise 3.210. Let V be a vector space (over $\mathbb{R}$, say). Show that V is finite-dimensional iff there is no strictly increasing sequence of vector subspaces $W_0 \subsetneq W_1 \subsetneq \cdots \subseteq V$.

Many other familiar "basic" results in analysis and algebra also fail in the absence of at least DC.

Example 3.211. The following common situation does *not* require Choice, despite appearances. Given a function $f : X \to Y$ and an equivalence relation $\sim \subseteq X^2$, if $\forall x_1 \sim x_2\,(f(x_1) = f(x_2))$, then f descends to a function on the quotient set $\widetilde{f} : X/\!\sim \to Y$, defined by $\widetilde{f}([x]) := f(x)$.

It may appear that we are "choosing an arbitrary representative x from the equivalence class"; however, because the choice doesn't matter, we can simply define $\widetilde{f}$ via comprehension:

$$\begin{aligned}\widetilde{f} &:= \{(C, y) \in X/\!\sim \times Y \mid \exists x \in C\,(f(x) = y)\} \\ &= \{(C, y) \in X/\!\sim \times Y \mid \forall x \in C\,(f(x) = y)\}.\end{aligned}$$

Exercise 3.212. Show that full Choice is equivalent to: every surjection $f : X \twoheadrightarrow Y$ has a section (right inverse) $g : Y \hookrightarrow X$.

Exercise 3.213. Show that the following statement is equivalent to full Choice. For any set X, set I, sets $(J_i)_{i\in I}$, and sets $(A_{i,j} \subseteq X)_{i\in I, j\in J_i}$,

$$\bigcap_{i\in I} \bigcup_{j\in J_i} A_{i,j} = \bigcup_{(j_i)_{i\in I} \in \prod_{i\in I} J_i} \bigcap_{i\in I} A_{i,j_i}.$$

[It suffices to consider $X = 1$.] Similarly, for a set I, sets $(J_i)_{i\in I}$, and reals $(x_{i,j} \in [0,1])_{i\in I, j\in J_i}$,

$$\inf_{i\in I} \sup_{j\in J_i} x_{i,j} = \sup_{(j_i)_{i\in I} \in \prod_{i\in I} J_i} \inf_{i\in I} x_{i,j_i}.$$

Returning to our original motivating intro to this subsection: a large class of applications of Choice, or rather the well-ordering theorem, consists of inductively constructing objects satisfying various constraints. Roughly speaking, the general format of such constructions is: if all the constraints are *finitary* in nature, and *finitely consistent* with each other, then they can always be satisfied.

Theorem 3.214. Let X be a set, $R \subseteq X^2$ be a directed graph (i.e., binary relation). Then there is a maximal R**-clique** $A \subseteq X$, i.e., $A^2 \subseteq R$.

Proof. Fix a well-order $< \subseteq X^2$. Define $<$-inductively

$$A := \{x \in X \mid x \mathrel{R} x \ \&\ \forall A \ni y < x \, (x \mathrel{R} y \mathrel{R} x)\}.$$

(That is, define inductively the indicator function $f : X \to 2$ of A by

$$f(x) = 1 \ :\iff \ x \mathrel{R} x \ \&\ \forall y < x \, (f(y) = 1 \implies x \mathrel{R} y \mathrel{R} x),$$

and then put $A := f^{-1}(1)$.) Then $A^2 \subseteq R$ by construction. To show maximality: if $x \in X \setminus A$, then either $x \not\mathrel{R} x$ in which case $A \cup \{x\}$ is not a clique, or there is $A \ni y < x$ such that $x \not\mathrel{R} y$ or $y \not\mathrel{R} x$ in which case again $A \cup \{x\}$ is not a clique; thus x cannot be added to A while keeping it a clique. □

Corollary 3.215 (Hausdorff maximality principle)**.** Every poset $(X, \leq)$ has a maximal linearly ordered subset. □

Corollary 3.216 (Zorn's lemma)**.** Let $(X, \leq)$ be a poset such that every linearly ordered subset has an upper bound. Then X has a maximal element.

Proof. Let $C \subseteq X$ be maximal linearly ordered, u be an upper bound of it. Then u is maximal, since if $v \geq u$, then v is also an upper bound of C, whence $v \in C$ by maximality, whence $v \leq u$. □

Exercise 3.217. Show (over ZF) that Zorn's lemma implies Choice. Thus the preceding three results are all equivalent to Choice.

Zorn's lemma is frequently used in "ordinary" math outside of logic, often in proofs that have the flavor of transfinite/well-ordered induction (but do not require knowing what these words mean). The following generalization of Theorem 3.214 is a typical example; we give two proofs.

Theorem 3.218. Let X be a set, $R_n \subseteq X^n$ for each $n \in \mathbb{N}$ be a family of finitary relations (a "directed hypergraph"). Then there is a maximal $A \subseteq X$ such that $A^n \subseteq R_n$ for each n.

Proof 1. Consider the poset of all such A, ordered by inclusion. If $C \subseteq \mathcal{P}(X)$ is a linearly ordered set of such A, then $\bigcup C$ is also such an A, i.e., $(\bigcup C)^n \subseteq R_n$ for each n, since for any $\vec{x} = (x_0, \ldots, x_{n-1}) \in (\bigcup C)^n$, each $x_i \in A_i$ for some $A_i \in C$, whence the largest A_i contains all of $x_0, \ldots, x_{n-1}$, whence $\vec{x} \in A_i^n \subseteq R_n$. Now apply Zorn's lemma. □

Proof 2. Fix a well-order $< \subseteq X^2$. As in Theorem 3.214, define inductively

$$A := \{x \in X \mid \forall n \in \mathbb{N} \forall y_0, \ldots, y_{n-1} \leq x \, (\forall i < n \, (y_i < x \implies y_i \in A) \implies \vec{y} \in R_n)\}.$$

Then $A^n \subseteq R_n$ for each n: to show $\vec{y} \in A^n$ is in R_n, apply the definition of A to $x = \max_{i<n} y_i$. To show maximality: if $x \notin A$, then there are $n \in \mathbb{N}$ and $y_0, \ldots, y_{n-1} \leq x$ such that each $y_i < x$ is in A but $\vec{y} \notin R_n$; then $\vec{y} \in (A \cup \{x\})^n$, so we cannot add x to A while maintaining $A^n \subseteq R_n$. □

Corollary 3.219. Every vector space V over every field K has a basis, i.e., a maximal linearly independent set $B \subseteq V$.[24]

Proof. B is linearly independent iff for each $n \in \mathbb{N}$, B^n is contained in the set of n-tuples of vectors with no nontrivial zero linear combination. □

[24] A theorem of Andreas Blass shows that this is equivalent over ZF to Choice!

Corollary 3.220. There exists a function $f : \mathbb{R} \to \mathbb{R}$ such that

$$f(x+y) = f(x) + f(y) \quad \forall x, y \in \mathbb{R},$$

yet f is not given by $f(x) = cx$ for any constant $c \in \mathbb{R}$.

Proof. Pick a $\mathbb{Q}$-basis $B \subseteq \mathbb{R}$ and define the $\mathbb{Q}$-linear transformation f by scaling basis elements by different amounts. □

Can you think of such a function? The following theorem is well beyond the scope of this course:

Theorem 3.221. It is not possible to explicitly define any such function $f : \mathbb{R} \to \mathbb{R}$. More precisely:

(a) It is not possible[25] to prove from $\mathsf{ZF} + \mathsf{DC}$ that any such function exists.
(b) It *is* possible to explicitly define such a function $f : \mathbb{R}^L \to \mathbb{R}$ on a $\mathbb{Q}$-linear subspace $\mathbb{R}^L \subseteq \mathbb{R}$. Thus by (a), it is not possible to prove in $\mathsf{ZF} + \mathsf{DC}$ that $\mathbb{R}^L = \mathbb{R}$. Moreover, it is also not possible to prove, even in ZFC, that $\mathbb{R}^L \neq \mathbb{R}$.

In other words, not only can you not define such an f, but you cannot even prove that you cannot define such an f! (Exercise: do the two uses of "define" here mean the same thing?)

The above is one among many results illustrating the "non-constructive" nature of Choice:

Theorem 3.222 (prime ideal theorem)**.** Let $(R, +, 0, \cdot, 1)$ be a **commutative rig**, i.e., a set equipped with two commutative, associative, and unital operations, such that $\cdot$ distributes over $+$. Let $F \subseteq R$ be a **multiplicative submonoid**, i.e., closed under $\cdot, 1$, and $I \subseteq R$ be an **ideal**, i.e., closed under $+, 0$, and $r \cdot (-)$ for each $r \in R$. Suppose $F \cap I = \varnothing$. Then there is an ideal $I \subseteq J \subseteq R$ which is **prime**, meaning $R \setminus J$ is a multiplicative submonoid, such that $F \cap J = \varnothing$.

Proof. Consider the poset of all ideals $I \subseteq J \subseteq R$ such that $F \cap J = \varnothing$. For a linearly ordered set C of such J, $I \cup \bigcup C$ is still such an ideal: it clearly contains I and is disjoint from F; and it is still an ideal, because $\{I\} \cup C$ is linearly ordered and the definition of "ideal" involves being closed under some finitary conditions. Thus, by Zorn's lemma there is a maximal such J. It remains to show that $R \setminus J$ is a multiplicative submonoid. We have $1 \in R \setminus J$, since $1 \in F$ and $F \cap J = \varnothing$. Now let $a, b \in R \setminus J$. It is easily verified that

$$J + Ra := \{c + ra \mid c \in J \ \&\ r \in R\}$$

is an ideal, which contains J (take $r = 0$) and a (take $c = 0$ and $r = 1$), hence by maximality of J, $c + ra \in F$ for some $c \in J$, $r \in R$. Similarly, $d + sb \in F$ for some $d \in J$, $s \in R$. Then

$$\begin{aligned} F &\ni (c + ra)(d + sb) \\ &= cd + csb + rad + rasb \end{aligned}$$

where the first three terms are (multiples of c or d, hence) in J, whence $ab \in R \setminus J$ or else the last term is also in J, contradicting $F \cap J = \varnothing$. □

Corollary 3.223. There exists a function $u : \mathcal{P}(\mathbb{N}) \to 2$ preserving all finite Boolean operations and mapping every finite set to 0.

Such a function is called a **nonprincipal ultrafilter** on $\mathbb{N}$. Note that without the last restriction on finite sets, there are "trivial" such u: namely, for any $n \in \mathbb{N}$, we may map $A \subseteq \mathbb{N}$ to 1 iff $n \in A$. Thus, a nonprincipal ultrafilter can be thought of as a "generalized element" of $\mathbb{N}$.

Proof. Regard $\mathcal{P}(\mathbb{N})$ as a rig with $+ = \cup$ and $\cdot = \cap$. Then $u^{-1}(0)$ for the desired u will be a prime ideal in $\mathcal{P}(\mathbb{N})$; and conversely, it is easily verified that the indicator function of the complement of every prime ideal preserves finite Boolean operations. Now apply the prime ideal theorem to the ideal $I \subseteq \mathcal{P}(\mathbb{N})$ of finite sets, which is disjoint from the multiplicative submonoid $F = \{\mathbb{N}\}$. □

[25] assuming that ZF is consistent to begin with; otherwise everything is provable

Remark 3.224. Once again, it is not possible to explicitly define such u, nor to prove that this is impossible. Indeed, there is a common generalization underlying both this result and Theorem 3.221. Between any "reasonable" groups, such as $\mathbb{R}$ with addition, $\mathcal{P}(\mathbb{N})$ with symmetric difference, or 2 with XOR, any "definable" group homomorphism must be continuous!

For the next few applications, we introduce some terminology. Let X be a set and $\mathcal{A} \subseteq \mathcal{P}(X)$ a family of subsets. We say $\mathcal{A}$ has the **finite intersection property** if every finite $\mathcal{F} \subseteq \mathcal{A}$ has nonempty intersection. We call $\mathcal{A}$ **compact** if every $\mathcal{B} \subseteq \mathcal{A}$ with the finite intersection property must itself have nonempty intersection. Intuitively, we think of each $A \in \mathcal{A}$ as a "constraint"; compactness means that every family of "finitely consistent" constraints can be satisfied.

Corollary 3.225 (Alexander subbasis lemma)**.** Let X be a set, $\mathcal{A} \subseteq \mathcal{P}(X)$ be a set of subsets. If $\mathcal{A}$ is compact, then so is the set $\mathcal{C}$ of finite unions of sets in $\mathcal{A}$.[26]

Proof. Let $\mathcal{D} \subseteq \mathcal{C}$ have the finite intersection property. Then the closure $\mathcal{D}'$ of $\mathcal{D}$ under finite intersections is disjoint from the ideal $\{\varnothing\} \subseteq \mathcal{P}(X)$, hence there is a prime ideal $\mathcal{J} \subseteq \mathcal{P}(X)$ disjoint from $\mathcal{D}'$, hence from $\mathcal{D}$. Each set $D \in \mathcal{D} \subseteq \mathcal{C}$, being a finite union of sets in $\mathcal{A}$, must contain at least one set in $\mathcal{A} \setminus \mathcal{J}$, or else D would be in $\mathcal{J}$ since $\mathcal{J}$ is an ideal. Thus $\bigcap \mathcal{D} \supseteq \bigcap(\mathcal{A} \setminus \mathcal{J}) \neq \varnothing$, since $\mathcal{A} \setminus \mathcal{J} \subseteq \mathcal{A}$ has the finite intersection property, since $\mathcal{J}$ is a prime ideal. □

Theorem 3.226 (Tychonoff for 2)**.** Let I be a set, $\mathcal{C} \subseteq \mathcal{P}(2^I)$ be the set of **clopen sets**, i.e., those $C \subseteq 2^I$ such that membership in C depends only on finitely many coordinates. Then $\mathcal{C}$ is compact.[27]

Proof. To say that membership in C depends only on the finitely many coordinates $I' \subseteq I$ means that for some $C' \subseteq 2^{I'}$, we have

$$C = \{x \in 2^I \mid x|I' \in C'\} = \bigcup_{x' \in C'} \overbrace{\{x \in 2^I \mid x' \subseteq x\}}^{A_{x'} :=}.$$

Thus letting $\mathcal{A} := \{A_{x'} \mid I' \subseteq I \text{ finite } \&\ x' \in 2^{I'}\}$, $\mathcal{C}$ consists of finite unions of sets in $\mathcal{A}$. Thus, it suffices to show $\mathcal{A}$ is compact. Let $\mathcal{B} \subseteq \mathcal{A}$ have the finite intersection property. For each $A_{x'} \in \mathcal{B}$, x' is a partial function $I \to 2$ with finite domain; and for two such $A_{x'}, A_{x''} \in \mathcal{B}$, the finite intersection property ensures that $A_{x'} \cap A_{x''} \neq \varnothing$, whence x', x'' agree on the intersection of their domains. Thus

$$x := \bigcup\{x' \in 2^{I'} \mid I' \subseteq I \text{ finite } \&\ A_{x'} \in \mathcal{B}\}$$

is a partial function $I \to 2$; extending it arbitrarily to the rest of I yields an element of $\bigcap \mathcal{B}$. □

This result is known to be weaker than full Choice. Intuitively, it provides a way to build objects satisfying finitary constraints and consisting only of *finitary data* (bits in 2). For example:

Corollary 3.227. There exists a function $f : 2^{\mathbb{N}} \to 2$ preserving bitwise XOR and mapping every infinite bit string with exactly one 1 to 1.

In other words, this is a linear transformation over the field $\mathbb{F}_2$ with 2 elements, hence follows easily from Corollary 3.219. But we can also deduce it as follows:

Proof. For $f \in 2^{2^{\mathbb{N}}}$ to obey the specified conditions means (i) $f(u \oplus v) = f(u) \oplus f(v)$ for all $u, v \in 2^{\mathbb{N}}$, and (ii) $f(\delta_i) = 1$ for all $i \in \mathbb{N}$ where $\delta_i(j) = 1 :\iff i = j$. The set of f obeying (i) for fixed u, v is a clopen set depending on coordinates $u, v, u \oplus v \in 2^{\mathbb{N}}$, while the set of f obeying (ii) for fixed i is a clopen set depending on coordinate $\delta_i \in 2^{\mathbb{N}}$; thus by Tychonoff, it suffices to show any finitely many of these conditions can be satisfied. Consider the finite-dimensional $\mathbb{F}_2$-subspace $V \subseteq 2^{\mathbb{N}}$ spanned by the u, v, δ_i mentioned in these conditions; define linear $f : V \to 2$ to map the linearly independent vectors δ_i to 1, and extend by linearity to all of V using finite-dimensional linear algebra; and then extend f to an arbitrary function on all of $2^{\mathbb{N}}$ (possibly nonlinear). □

[26] In other words, a topological space is compact if every *subbasic* open cover has a finite subcover.

[27] Also known as the compactness theorem for propositional logic.

Exercise 3.228. Use Tychonoff's theorem for 2 to show that Theorem 3.222 holds for every powerset (this is known as the **Boolean prime ideal theorem**). Thus, the following are equivalent over ZF, and all weaker than full Choice:

- the Boolean prime ideal theorem;
- the Alexander subbasis lemma;
- Tychonoff's theorem for 2.

In fact, Tychonoff's theorem for arbitrary products of finite sets is also equivalent. (This even works for products of compact Hausdorff spaces; but the proof there is more involved.)

Exercise 3.229 (for topologists)**.**

(a) Using the Alexander subbasis lemma, prove the full Tychonoff's theorem: every product of compact topological spaces is compact.

(b) Prove that Tychonoff's theorem implies Choice. [To choose elements from sets X_i, consider topological spaces of the form $X_i \sqcup \{\top\}$, where $\top$ is an additional element, with topologies consisting of at most 3 open sets.]

(Thus, (a) must in fact also use full Choice, aside from the Alexander subbasis lemma.)

Our final group of applications of Choice are of a more geometrical nature:

Theorem 3.230 (Vitali)**.** Let $S^1 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$ be the unit circle. There is a way to partition $S^1 = A_0 \sqcup A_1 \sqcup \cdots$ into countably many subsets, slide those subsets around in the plane (i.e., using translations and rotations), and rearrange them into two disjoint unit circles.

Proof. Consider the equivalence relation $\sim$ on S^1 defined by $\vec{v} \sim \vec{w} :\iff$ the angle between them is rational (in degrees, i.e., a rational multiple of 2π). Let $C \subseteq S^1$ choose exactly one element from each equivalence class. For each $r \in \mathbb{Q}/\mathbb{Z}$, let C_r be the rotation of C by $2\pi r$; then

$$S^1 = \bigsqcup_{r \in \mathbb{Q}/\mathbb{Z}} C_r$$

is the desired countable partition. To see this works: note that any two C_r, C_s may be rotated onto each other. Thus for any infinite $R \subseteq \mathbb{Q}/\mathbb{Z}$, finding a bijection $f : R \cong \mathbb{Q} \cap [0, 1)$, we may move the pieces C_r for $r \in R$ to another complete copy of S^1, by rotating each C_r to $C_{f(r)}$. Finally, find a partition $\mathbb{Q}/\mathbb{Z} = R \sqcup S$ into two infinite sets; move C_r for $r \in R$ into one copy of S^1; and move C_s for $s \in S$ into another copy. □

Exercise 3.231. In fact, S^1 may be rearranged into countably many copies of S^1.

Remark 3.232. Theorem 3.230 is the main ingredient in a basic result in measure theory: that it is not possible to define a meaningful notion of "length" for every subset of $\mathbb{R}$ or S^1. If this were possible, then the pieces in the above partition used to make the first copy of S^1 would have total length 2π, as would the pieces in the second copy; but their total length would also be 2π.

More precisely, there cannot be a notion of "length" $\mu : \mathcal{P}(S^1) \to \mathbb{R}$ obeying some intuitively reasonable axioms that were used in the above argument. Namely, μ should always be nonnegative; $\mu(S^1) = 2\pi$; μ should be preserved under rotations; and μ should add over countable partitions. This last requirement may seem a little fishy; after all, we cannot require μ to add over *arbitrary* partitions, since S^1 is an uncountable union of singletons. What if we allow only finite partitions?

Theorem 3.233 (Banach)**.** There exists a function $\mu : \mathcal{P}(S^1) \to [0, 2\pi]$ such that $\mu(S^1) = 2\pi$, μ is preserved under rotations, and $\mu(A \cup B) = \mu(A) + \mu(B)$ for all disjoint $A, B \subseteq S^1$. (Such a μ is called an **invariant finitely additive measure**.) Thus, it is not possible to break S^1 into *finitely* many pieces and rearrange them to form two copies of S^1.

Proof. First, we show that for any finite set of angles $F \subseteq \mathbb{R}$ and $\varepsilon > 0$, we can find a μ which is preserved under rotations by only these angles and only up to an error of ε. That is, if $A \subseteq S^1$, $r \in F$, and $A' = A$ rotated by $2\pi r$, then $|\mu(A) - \mu(A')| \leq \varepsilon$. We will define μ by

$$\mu(A) := \frac{2\pi \left|\{(a_r)_{r\in F} \in N^F \mid (\cos(2\pi \sum_{r\in F} a_r r), \sin(2\pi \sum_{r\in F} a_r r)) \in A\}\right|}{N^{|F|}}$$

for $2\pi/\varepsilon \leq N \in \mathbb{N}$. In other words, instead of the actual length of A, we only sample along points at angles $2\pi \sum_{r\in F} a_r r$ where the coefficients run up to N, and take the proportion of these points which are in A. If we rotate A by r, each point in A with $a_r < N-1$ will correspond to a point in the rotated A' with a_r increased by 1. Thus the membership status of at most $N^{|F|-1}$ points (those with $a_r = N-1$, and arbitrary values $a_s \in N$ for $s \neq r$) can change, and so

$$|\mu(A) - \mu(A')| \leq \frac{2\pi N^{|F|-1}}{N^{|F|}} = \frac{2\pi}{N} \leq \varepsilon.$$

It is easily seen that also $\mu(S^1) = 2\pi$ and μ adds over disjoint unions.

Now for each finite $F \subseteq \mathbb{R}$ and $\varepsilon > 0$, the set of all functions $\mu : \mathcal{P}(S^1) \to [0, 2\pi]$ obeying the above conditions is a closed set $M_{F,\varepsilon} \subseteq [0, 2\pi]^{\mathcal{P}(S^1)}$. We have $M_{F,\varepsilon} \cap M_{F',\varepsilon'} \supseteq M_{F\cup F',\min(\varepsilon,\varepsilon')}$; thus the family of all $M_{F,\varepsilon}$ obeys the finite intersection property. Their intersection is the set of invariant finitely additive measures. By Heine–Borel (Theorem 3.31) and Tychonoff's theorem (Exercise 3.229), $[0, 2\pi]^{\mathcal{P}(S^1)}$ is compact, thus an invariant finitely additive measure exists. □

It turns out that this result is specific to low dimensions:

Theorem 3.234 (Banach–Tarski)**.** Let $S^2 = \{(x, y, z) \in \mathbb{R}^3 \mid x^2 + y^2 + z^2 = 1\}$ be the unit sphere. There is a way to partition S^2 into finitely many subsets, slide those subsets around using translations and (3D) rotations, and rearrange them into two disjoint unit spheres.

What is the precise connection between this result and Theorems 3.230 and 3.233? All three results are really about *transformation groups*: the group of all rotations of S^1 in the case of the former theorems, which is isomorphic to $\mathbb{R}/\mathbb{Z}$ under $+$; and the group $\mathrm{SO}(3)$ of rotations of S^2, i.e., 3×3 orthogonal matrices, in the case of the Banach–Tarski Theorem 3.234.

In Theorem 3.230, we took a countable subgroup of $\mathbb{R}/\mathbb{Z}$, namely the rational ones $\mathbb{Q}/\mathbb{Z}$. This group acts *freely* on S^1: for any $\vec{v} \in S^1$, $(r \mapsto$ rotation of $\vec{v}$ by $2\pi r)$ is a bijection between $\mathbb{Q}/\mathbb{Z}$ and the orbit of $\vec{v}$. Thus, after choosing a set C of representatives from each orbit, we get a bijection

$$\begin{aligned} C \times \mathbb{Q}/\mathbb{Z} &\cong S^1 \\ (\vec{v}, r) &\mapsto \text{rotation of } \vec{v} \text{ by } 2\pi r \end{aligned}$$

such that rotation in S^1 corresponds to $+$ in the second coordinate $\mathbb{Q}/\mathbb{Z}$. Now the proof of Theorem 3.230 amounts to the trivial fact that $\mathbb{Q}/\mathbb{Z}$, being countable, may be partitioned into

$$\mathbb{Q}/\mathbb{Z} = \bigsqcup_{r\in\mathbb{Q}/\mathbb{Z}} \{r\}$$

such that these pieces may then be moved around in $\mathbb{Q}/\mathbb{Z}$ into two copies of $\mathbb{Q}/\mathbb{Z}$ (namely those in the sets R and S). By doing this rearrangement in the second coordinate of $C \times \mathbb{Q}/\mathbb{Z}$, the above bijection then yields the desired decomposition of S^1.

Theorem 3.233 thus implies that it is impossible to rearrange $\mathbb{Q}/\mathbb{Z}$ into two copies of itself via a *finite* partition. In fact, the proof of Theorem 3.233 shows this directly; simply replace $\mathbb{R}$ and "rotation" in that proof by $\mathbb{Q}/\mathbb{Z}$ and "addition". What that proof really shows is the following:

Theorem 3.235 (Banach)**.** For any abelian group $(G, +, 0, -)$, there exists an **invariant finitely additive probability measure** $\mu : \mathcal{P}(G) \to [0, 1]$ such that $\mu(G) = 1$, $\mu(A \sqcup B) = \mu(A) + \mu(B)$, and $\mu(A + g) = \mu(A)$ for any $A, B \subseteq G$ and $g \in G$.

The Banach–Tarski Theorem 3.234 thus depends crucially on the fact that SO(3) is *highly nonabelian*; in fact, in some sense, it is as complicated a group as possible:

Definition 3.236. The **free group on two generators** $\mathbb{F}_2 = \langle a, b \rangle$ consists of all finite strings (including empty) of the four symbols a, b, a^{-1}, b^{-1}, such that no letter occurs consecutively with its inverse. Two such strings are multiplied by concatenation followed by cancelling inverses: e.g.,

$$(aba^{-1}bb)(\cancel{b^{-1}}ab) = aba^{-1}bab.$$

In other words, $\mathbb{F}_2$ is obtained by "declaring there to be two elements a, b, and taking all elements built from those, with no relations between them except those implied by the group axioms".

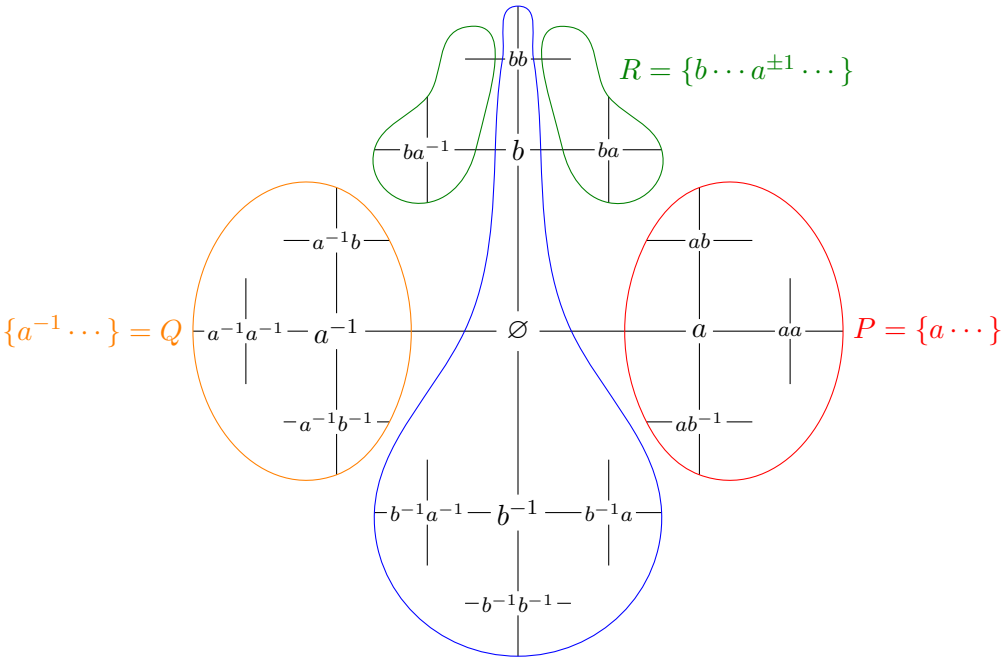
Theorem 3.237 (Hausdorff)**.** There are two orthogonal matrices $A, B \in \mathrm{SO}(3)$ obeying no relations not implied by the group axioms, i.e., such that we have an injective group homomorphism

$$\begin{aligned} \mathbb{F}_2 &\longrightarrow \mathrm{SO}(3) \\ a^{n_0}b^{n_1}a^{n_2}\cdots &\longmapsto A^{n_0}B^{n_1}A^{n_2}\cdots. \end{aligned}$$

This is the key technical ingredient underlying the Banach–Tarski paradox, and its proof involves numerical computations with matrices: for example, one could take the rotations about the x- and y-axes, both by the angle $\arcsin(\frac{3}{5})$ in a 3-4-5 right triangle, yielding matrices with rational entries.

Theorem 3.238. There is a finite partition $\mathbb{F}_2 = P \sqcup Q \sqcup R \sqcup S$ such that $\mathbb{F}_2 = P \sqcup aQ = R \sqcup bS$.

Proof.



□

Proof sketch of Banach–Tarski Theorem 3.234. We identify $\mathbb{F}_2$ with a subgroup of SO(3) via Theorem 3.237. Each nonidentity rotation $I_3 \neq T \in \mathrm{SO}(3)$ fixes only two points on S^3. Thus, there are countably many points $F \subseteq S^3$ such that every nonidentity $T \in \mathbb{F}_2$ moves every point in $S^3 \setminus F$; we will prove the weaker statement that $S^3 \setminus F$ can be countably partitioned and then rearranged into two copies of itself. Let $C \subseteq S^3 \setminus F$ choose exactly one point from each $\mathbb{F}_2$-orbit. Then

$$S^3 \setminus F = PC \sqcup QC \sqcup RC \sqcup SC$$

is the desired partition; indeed, PC, QC can be rearranged into one copy $S^3 \setminus F = PC \sqcup aQC$, while RC, SC can be rearranged into another copy $S^3 \setminus F = RC \sqcup bSC$. □

4. Cardinality

4.A. **Equinumerosity and cardinality.**

Definition 4.1. Two sets A, B are **equinumerous** or **have the same cardinality**, denoted

$$A \cong B,$$

if there exists a bijection $f : A \cong B$.

Remark 4.2. This is a (proper class) equivalence relation on V, since bijections are closed under composition, inversion, and identity.

The concept of equinumerosity is more fundamental than that of "the cardinality" $|A|$ of a set. We would like to define the latter to mean any object we can assign to A, in such a way that equinumerosity indeed means "having the same cardinality". For an equivalence relation on a set, we would just take the quotient; but equinumerosity is on the proper class V.

Definition 4.3 (assuming Foundation)**.** The **cardinality** $|A|$ of a set A is defined using Scott's trick (3.199), i.e., as the set of all sets equinumerous with A with minimal rank among all such sets.

Thus, a **cardinal** κ is a maximal nonempty set of equinumerous sets of equal rank.

Definition 4.4 (assuming Choice)**.** Then in each $\cong$-equivalence class, there is at least one ordinal; and among those, we may canonically choose the least one. The **cardinality** $|A|$ of a set A is the least ordinal equinumerous with A.

Thus, a **cardinal** κ is an **initial ordinal**: one not equinumerous with any strictly smaller ordinal.

As with other coding choices (Sections 2.D and 2.E), in ZFC (so both Foundation and Choice), the choice of which of these we call "cardinals" is largely irrelevant for ordinary mathematical practice. All we need to know is that

(4.5) For each set A, we have an object $|A|$ called its cardinality.
(4.6) Two sets have the same cardinality iff they are equinumerous.

Nonetheless, in the presence of Choice, the initial ordinals representation is somehow much more canonical and convenient, in the same way that the standard encoding of naturals is well-justified via the Mostowski collapse (see Example 3.138). Indeed, even in the absence of Choice, it makes sense to isolate the **well-orderable** cardinals (i.e., cardinalities of well-orderable sets) as special ones, and then to represent these via initial ordinals (while using some other representation such as Scott's trick for other cardinals).

4.B. **Cardinal comparison.**

Definition 4.7. A set A **injects** into another set B, denoted

$$A \hookrightarrow B,$$

if there exists an injection $f : A \hookrightarrow B$.

Remark 4.8. This is a preorder on V, since injections are closed under composition and identity.

Remark 4.9. $A \cong B \implies A \hookrightarrow B \hookrightarrow A$, since bijections are injections.

It follows from both of these properties that $A' \cong A \hookrightarrow B \cong B' \implies A' \hookrightarrow B'$, justifying

Definition 4.10. For two cardinals $|A|, |B|$,

$$|A| \leq |B| \ :\iff \ A \hookrightarrow B.$$

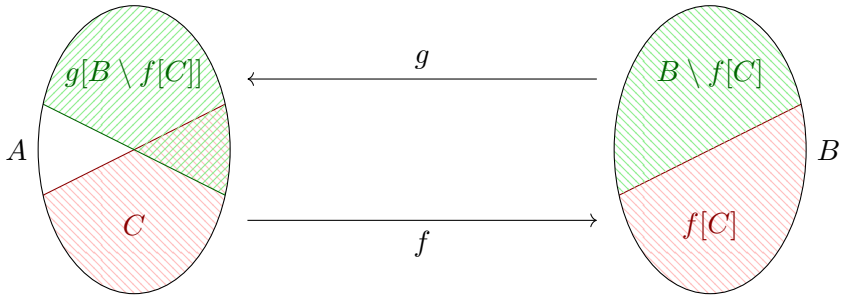
This is a preorder on the class of all cardinals (however we choose to encode them).

Theorem 4.11 (Schröder–Bernstein)**.** For any two sets A, B, if $A \hookrightarrow B \hookrightarrow A$, then $A \cong B$.

Thus $\leq$ on cardinals is a partial order.

Proof. Let $f : A \hookrightarrow B$ and $g : B \hookrightarrow A$; our goal is to construct a bijection $h : A \cong B$ which is equal to f on some elements and g^{-1} on others (or possibly both). Let $C \subseteq A$ be the elements on which it's given by f. Then part of h will be given by the bijection $f : C \cong f[C] \subseteq B$. The rest must be given by the inverse of $g : B \setminus f[C] \cong g[B \setminus f[C]] \subseteq A$; thus we must find $C \subseteq A$ such that

$$C = A \setminus g[B \setminus f[C]].$$



Since $C \mapsto A \setminus g[B \setminus f[C]]$ is monotone, by Knaster–Tarski such a fixed point C exists. □

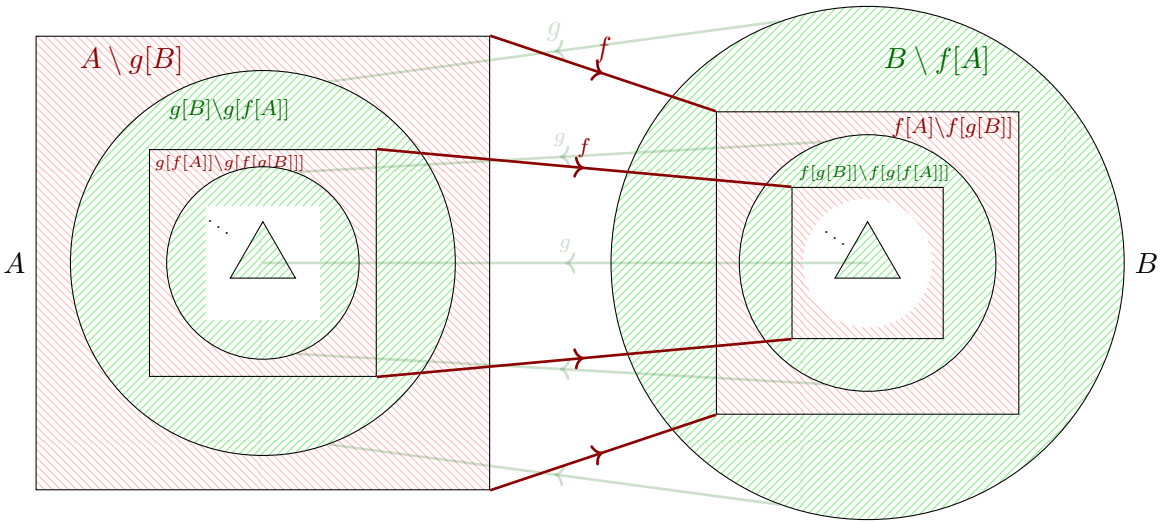
Remark 4.12. For a more informative proof, we may use the transfinite version of Knaster–Tarski 3.176. Note also that since g is injective, we may write the above operator more intelligibly as

$$\begin{aligned} A \setminus g[B \setminus f[C]] &= A \setminus (g[B] \setminus g[f[C]]) \\ &= (A \setminus g[B]) \sqcup g[f[C]], \end{aligned}$$

which is clearly finitary (indeed unary); thus by Proposition 3.180, the least fixed point $C \subseteq A$ is the union of the first ω iterates (again using that $g \circ f$ is injective)

$$\begin{aligned} \varnothing &\subseteq A \setminus g[B] \\ &\subseteq (A \setminus g[B]) \sqcup (g[f[A]] \setminus g[f[g[B]]]) \\ &\subseteq (A \setminus g[B]) \sqcup (g[f[A]] \setminus g[f[g[B]]]) \sqcup (g[f[g[f[A]]]] \setminus g[f[g[f[g[B]]]]]) \\ &\subseteq \cdots . \end{aligned}$$

This union consists of the red rings on the left below; the resulting bijection h simply switches each with the green ring inside it, while applying g^{-1} on the remaining "center".



Exercise 4.13. Verify that if we instead take the greatest fixed point C of $C \mapsto A \setminus g[B \setminus f[C]]$, the bijection h is defined the same way as above except being given by f instead of g^{-1} on the "center".

Remark 4.14. Are the cardinals *linearly* ordered? This is equivalent to Choice; see Corollary 4.24.

4.C. **Well-orderable cardinals.**

Proposition 4.15. For an ordinal α and initial ordinal κ, we have $\kappa \subseteq \alpha \iff \kappa \hookrightarrow \alpha$.

In other words, an initial ordinal is (not only not equinumerous with but) does not inject into any smaller ordinal.

In particular, ordinal and cardinal comparison agree on initial ordinals.

Proof. Clearly, $\kappa \subseteq \alpha \implies \kappa \hookrightarrow \alpha$. Conversely, if $\kappa \not\subseteq \alpha$, then since ordinals are linearly ordered, $\alpha \subsetneq \kappa$; since κ is initial, this means $\alpha \not\cong \kappa$, whence $\kappa \not\hookrightarrow \alpha$ by Schröder–Bernstein. □

Theorem 4.16 (pigeonhole principle)**.** For $m, n \in \mathbb{N}$, we have $m \leq n \iff m \hookrightarrow n$.

In other words, naturals are initial ordinals.

Proof. By induction on n. If $n = 0$, then clearly $m \hookrightarrow n = \varnothing$ implies $m = \varnothing$. Now suppose every $m \hookrightarrow n$ is $\leq n$, and let $f : m \hookrightarrow n + 1$. If $m = 0$, then clearly $m \leq n$. Now suppose $m > 0$, whence $m = m' + 1$ for some $m' \in \mathbb{N}$. If $f[m'] \subseteq n$, then by the IH, $m' \leq n$, whence $m = m' + 1 \leq n + 1$. Otherwise, there is some $k < m'$ such that $f(k) = n$, whence since f is injective, $f(m') < n$; modify f by swapping $f(k), f(m')$, and apply the previous case. □

Proposition 4.17. If K is a set of initial ordinals, then $\sup K \in \mathbb{ON}$ is initial.

Proof. If $\sup K \hookrightarrow \alpha < \sup K$, then $\alpha < \kappa$ for some $\kappa \in K$, and $\kappa \leq \sup K \hookrightarrow \alpha$, contradicting that κ is initial. □

Corollary 4.18. ω is an initial ordinal: $\omega \not\hookrightarrow n$ for all $n \in \omega$. □

Theorem 4.19 (Hartogs)**.** For every set A, there is a (least) ordinal $\eta(A)$, called the **Hartogs number** of A, that does not inject into A.

Note that $\eta(A)$ is then clearly initial.

Proof. If $\alpha \in \mathbb{ON}$ injects into A, then α is the rank of a well-order on a subset of A (namely the image of the injection). Thus $\eta(A) = \operatorname{mex}\{\rho_<[B] \mid B \subseteq A \ \&\ < \text{ is a well-order on } B\}$. □

Corollary 4.20. For every initial ordinal κ, there is a least initial ordinal $> \kappa$, called the **successor cardinal** $\kappa^+ = \eta(\kappa)$.

Note that this is not to be confused with the successor ordinal (Proposition 3.149). For naturals they agree, but otherwise κ^+ is much bigger:

Example 4.21. The successor cardinal ω^+ is the smallest uncountable ordinal, usually denoted ω_1.

Definition 4.22. $\aleph_\alpha = \omega_\alpha$ is the αth infinite initial ordinal. Thus

$$\begin{aligned}
\aleph_0 &= \omega_0 = \omega,\\
\aleph_1 &= \omega_1 = \omega^+,\\
\aleph_2 &= \omega_2 = \omega^{++},\\
&\vdots\\
\aleph_\omega &= \sup\nolimits_{n<\omega} \aleph_n \quad \text{by Proposition 4.17;}
\end{aligned}$$

more generally,

$$\begin{aligned}
\aleph_{\alpha+1} &= \aleph_\alpha^+,\\
\aleph_\alpha &= \sup\nolimits_{\beta<\alpha} \aleph_\beta \quad \text{for limit ordinals } \alpha\text{, by Proposition 4.17.}
\end{aligned}$$

Remark 4.23. By Proposition 3.202(iii), every cardinal $\leq$ an initial ordinal is itself well-orderable.

Corollary 4.24 (over ZF)**.** The Axiom of Choice is equivalent to: cardinals are linearly ordered.

Proof. If Choice holds, then every cardinal is an initial ordinal, which are well-ordered.

Conversely, if a set A is comparable in cardinality with $\eta(A)$, then since $\eta(A) \not\hookrightarrow A$, $A \hookrightarrow \eta(A)$, whence A is well-orderable. □

Exercise 4.25. By essentially Proposition 3.202(iv), for a nonempty set A and well-ordered set B, we have $A \hookrightarrow B$ iff $B \twoheadrightarrow A$.

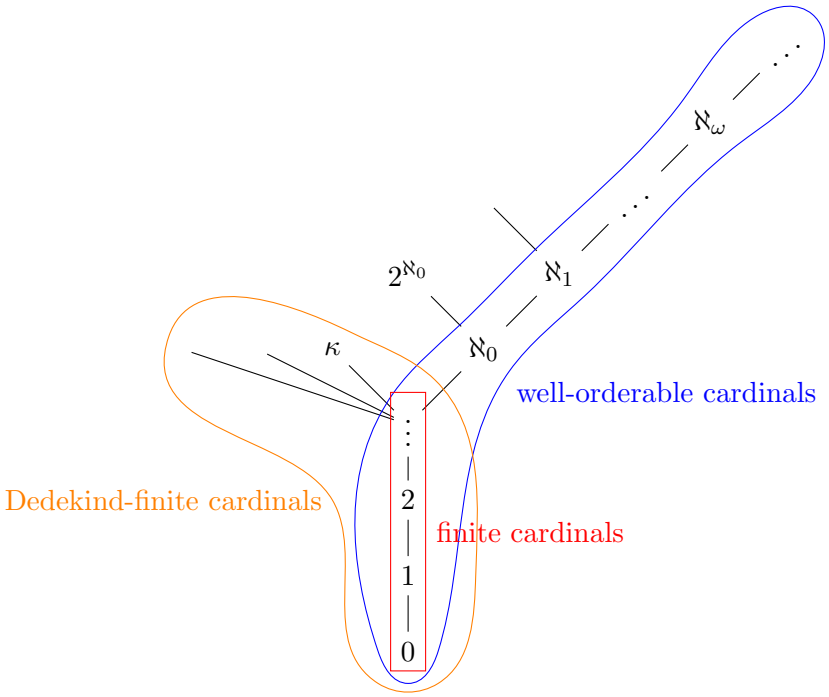
For example, this says that a nonempty set is countable ($A \hookrightarrow \mathbb{N}$) iff it has an enumeration.

Proposition 4.26. Every cardinal is comparable with every natural $n \in \mathbb{N}$.

Proof. By induction on n. Clearly $0 \hookrightarrow A$ for every set A. Now suppose n is comparable with $|A|$. If $A \hookrightarrow n$, then clearly $A \hookrightarrow n+1$. Otherwise, let $f : n \hookrightarrow A$. If f is surjective, then $f^{-1} : A \hookrightarrow n+1$. Otherwise, there exists $a \in A \setminus \mathrm{im}(f)$; extend f to $n+1$ by $f(n) := a$ to get $n+1 \hookrightarrow A$. □

We thus get the following picture of cardinals in the absence of Choice:

(4.27)



The well-orderable cardinals, i.e., initial ordinals, form a well-ordered (because $\mathbb{ON}$ is well-ordered), downward-closed (by Remark 4.23) "spine" without an upper bound (by Hartogs). Among them, the finite cardinals $n \in \omega$ form an "initial segment" that's actually below everything else (by Proposition 4.26). Above them, there could be infinite cardinals that are not $\geq \aleph_0$, i.e., cardinalities of infinite sets without an infinite sequence, since Dependent Choice is required to construct such an infinite sequence (Proposition 3.206); such sets are called infinite **Dedekind-finite**, and have Hartogs number $\aleph_0$. Similarly, even if DC holds, there could be uncountable cardinalities (not $\leq \aleph_0$, which means $> \aleph_0$ assuming DC) that are incomparable with $\aleph_1$.

Remark 4.28. In particular, $2^{\aleph_0}$, the cardinality of $\mathbb{R}$ (see Example 4.36), is usually considered to be "definably" incomparable with $\aleph_1$; for the precise meaning of this, take a course in descriptive set theory. Indeed, there is even a theorem saying that under some reasonable "definability" hypotheses, $\aleph_1$ and $2^{\aleph_0}$ are the only two minimal uncountable cardinalities!

4.D. **Cardinal arithmetic.** In general, given any (say binary) operation $*$ on sets which is *functorial* in the sense of Definition 2.68, functoriality implies that $*$ respects the equivalence relation $\cong$ on V, hence descends to an operation on the quotient class of cardinals defined via

$$|A| * |B| := |A * B|.$$

Definition 4.29. The **sum** of cardinals is induced by disjoint union (Definition 2.76):

$$|A| + |B| := |A \sqcup B| = \big|\{(i, x) \in 2 \times (A \cup B) \mid (i = 0 \ \&\ x \in A) \text{ or } (i = 1 \ \&\ x \in B)\}\big|.$$

Definition 4.30. The **product** of cardinals is induced by Cartesian product (Definition 2.32):

$$|A| \cdot |B| := |A \times B|.$$

Definition 4.31. Exponentiation of cardinals is induced by function sets (Definition 2.48):

$$|B|^{|A|} := \big|B^A\big|.$$

(Functoriality is by Example 2.71.)

Remark 4.32. For cardinals represented as initial ordinals κ, λ, these notions must not be confused with the ordinal arithmetic operations from Section 3.H with the same name!

For $+$ and $\cdot$, we at least have that the ordinal operation yields a (typically non-initial) ordinal whose cardinality is the cardinal operation:

$$|\text{ordinal } \kappa + \lambda| = \text{cardinal } \kappa + \lambda,$$
$$|\text{ordinal } \kappa \cdot \lambda| = \text{cardinal } \kappa \cdot \lambda.$$

These follow from the rank-based definitions of ordinal $+, \cdot$ from Exercise 3.169. It follows that

$$\text{ordinal } \kappa + \lambda \geq \text{cardinal } \kappa + \lambda,$$
$$\text{ordinal } \kappa \cdot \lambda \geq \text{cardinal } \kappa \cdot \lambda.$$

For exponentiation however, the ordinal power from Exercise 3.172 will usually be much smaller than the cardinal power! For example, the ordinal power $2^\omega = \sup\{1, 2, 4, 8, \dots\} = \omega$ is countable, whereas the cardinal power 2^ω is not, by Cantor's Theorem 2.9 (see also 4.35).

(Note that the cardinal operations *do* agree with ordinal ones on naturals, since these are all initial by Theorem 4.16.)

Just as any functorial set operation descends to an operation on cardinals, so does every natural bijection between two such operations (see Section 2.E) yield an algebraic identity:

Proposition 4.33. The following all refer to cardinal operations:

(a) $+$ and $\cdot$ are commutative and associative, with respective identity elements $0, 1$.
(b) $\cdot$ distributes over $+$ and $\kappa \cdot 0 = 0$. In particular, $\kappa \cdot n = \underbrace{\kappa + \cdots + \kappa}_{n}$ for $n \in \mathbb{N}$.
(c) $\kappa^{\lambda+\mu} = \kappa^\lambda \cdot \kappa^\mu$ and $\kappa^0 = 1$. In particular, $\kappa^n = \kappa \cdots \kappa$ for $n \in \mathbb{N}$.
(d) $(\kappa \cdot \lambda)^\mu = \kappa^\mu \cdot \lambda^\mu$ and $1^\mu = 1$.
(e) $(\kappa^\lambda)^\mu = \kappa^{\lambda \cdot \mu}$ and $\kappa^1 = \kappa$.
(f) $|\mathcal{P}(X)| = 2^{|X|}$.

Proof. By various canonical bijections. For example, (e) follows from Example 2.81. □

We also get various *in*equalities, derived from natural *in*jections:

Proposition 4.34. Again referring only to cardinal operations:

(a) $+, \cdot$ are monotone (in both arguments).
(b) $\kappa \leq \lambda \implies \kappa^\mu \leq \lambda^\mu$, and $\kappa \leq \lambda \implies \mu^\kappa \leq \mu^\lambda$, unless $\mu = \kappa = 0 < \lambda$.

Proof. Let $f : A \hookrightarrow B$; then for any C,

$$\begin{aligned} A \sqcup C &\longhookrightarrow B \sqcup C \\ (0,a) &\longmapsto (0, f(a)) \\ (1,c) &\longmapsto (1,c), \end{aligned} \qquad \begin{aligned} A \times C &\longhookrightarrow B \times C \\ (a,c) &\longmapsto (f(a),c), \end{aligned} \qquad \begin{aligned} A^C &\longhookrightarrow B^C \\ g &\longmapsto f \circ g, \end{aligned}$$

which shows $|A| + |C| \le |B| + |C|$, $|A| \cdot |C| \le |B| \cdot |C|$, and $|A|^{|C|} \le |B|^{|C|}$. To show $|C|^{|A|} \le |C|^{|B|}$:

- If $|B| = 0$, then $|A| = 0$ (since $A \hookrightarrow B$), so this is clear.
- If $|A| > 0$, then f has a retraction (left inverse) $g : B \twoheadrightarrow A$, mapping $f(a) \mapsto a$ and every other $b \in B \setminus f[A]$ to some arbitrary $a_0 \in A$. Then
$$\begin{aligned} C^A &\longhookrightarrow C^B \\ h &\longmapsto h \circ g. \end{aligned}$$
- If $|A| = 0 < |C|$, then C^A is a singleton while C^B is nonempty (take a constant).
- Finally, if $|C| = |A| = 0 < |B|$, the inequality is false: $0^0 = 1 \not\le 0 = 0^{|B|}$. □

Theorem 4.35 (Cantor)**.** For any cardinal κ, $\kappa < 2^\kappa$.

Proof. Letting $\kappa = |A|$, we have $A \hookrightarrow \mathcal{P}(A)$ by $a \mapsto \{a\}$, but $A \ncong \mathcal{P}(A)$ by Theorem 2.9. □

Example 4.36. We have

$$\begin{aligned} \mathbb{R} &\longhookrightarrow \mathcal{P}(\mathbb{Q}) \\ r &\longmapsto \{q \in \mathbb{Q} \mid q < r\}, \end{aligned} \qquad \begin{aligned} \mathcal{P}(\mathbb{N}) &\longhookrightarrow \mathbb{R} \\ A &\longmapsto \textstyle\sum_{n \in A} 10^{-n}, \end{aligned}$$

whence

$$|\mathbb{R}| \le |\mathcal{P}(\mathbb{Q})| = 2^{|\mathbb{Q}|} = 2^{\aleph_0} = 2^{|\mathbb{N}|} = |\mathcal{P}(\mathbb{N})| \le |\mathbb{R}|$$

and so by Schröder–Bernstein,

$$|\mathbb{R}| = |\mathbb{P}(\mathbb{N})| = 2^{\aleph_0} > \aleph_0.$$

Example 4.37. We have

$$2^{\aleph_0} \le 3^{\aleph_0} \le \cdots \le \aleph_0^{\aleph_0} \le (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0}$$

(the last step using that $\mathbb{N}^2$ is countable, e.g., by the injections $n \mapsto (n, 0)$ and $(m, n) \mapsto 2^m 3^n$). Thus by Schröder–Bernstein, these cardinals are all equal. For example, we get $|\mathbb{R}^{\mathbb{N}}| = |\mathbb{R}|$.

We may also define indexed versions of cardinal operations:

Definition 4.38. For a set I and family of sets $(A_i)_{i \in I}$, the **indexed sum and product** of cardinals are defined via

$$\begin{aligned} \textstyle\sum_{i \in I} |A_i| &:= \left|\bigsqcup_{i \in I} A_i\right|, \\ \textstyle\prod_{i \in I} |A_i| &:= \left|\prod_{i \in I} A_i\right|. \end{aligned}$$

Exercise 4.39. Check that these are well-defined, i.e., depend only on the cardinalities of the A_i,[28] assuming the Axiom of Choice (why?).

Remark 4.40. Again, for sum only, this is related to the indexed ordinal sum from Exercise 3.169:

$$|\text{ordinal } \textstyle\sum_{\gamma < \beta} \kappa_\gamma| = \text{cardinal } \sum_{\gamma < \beta} \kappa_\gamma \le \text{ordinal } \sum_{\gamma < \beta} \kappa_\gamma.$$

Exercise 4.41. Prove indexed analogs of Proposition 4.33. [See Exercises 3.169 and 3.172.]

Exercise 4.42. Prove indexed analogs of Proposition 4.34, assuming the Axiom of Choice (why?).

We will say more about these indexed operations in Section 4.F below.

[28] See Exercise 2.79. Indeed, they are even invariant under replacing I with an equinumerous copy, provided we also reindex the A_i's. More precisely, $\sum$ and $\prod$ are functorial on a category called $\int_{I \in \mathsf{Set}} \mathsf{Set}^I$.

4.E. **Well-ordered cardinal arithmetic.** While the above laws of cardinal arithmetic had fairly "structural" proofs, under Choice things become much more trivial:

Proposition 4.43. For every infinite well-orderable cardinal κ, we have $\kappa + 1 = \kappa$.

Proof. We have $\aleph_0 + 1 = \aleph_0$, i.e., there is a bijection

$$\begin{aligned} \omega \sqcup \{0\} &\cong \omega \\ (0, n) &\mapsto n + 1 \\ (1, 0) &\mapsto 0. \end{aligned}$$

Now since $\omega \leq \kappa$, we get a bijection $\kappa \sqcup \{0\} \cong \kappa$ which is the above together with the identity function on $\kappa \setminus \omega$. □

Corollary 4.44. Every infinite initial ordinal $\kappa = \aleph_\alpha$ is a limit ordinal.

Proof. For $\alpha < \kappa$, either $\alpha < \omega$ in which case $\alpha + 1 < \omega$ by definition of ω, or α is infinite in which case $|\alpha + 1| = |\alpha| + 1 = |\alpha| \leq \alpha < \kappa$ whence $\alpha + 1 < \kappa$ since κ is initial. □

Exercise 4.45. Show that in general (without Choice), for a cardinal κ, the following are equivalent:

(i) $\kappa + 1 = \kappa$.
(ii) κ is Dedekind-infinite, i.e., $\aleph_0 \leq \kappa$ (see (4.27)).
(iii) For any set A with $|A| = \kappa$, there is a non-surjective injection $A \hookrightarrow A$.

Proposition 4.46. Let I be a well-orderable set, $(A_i)_{i \in I}$ be a family of sets. Then

$$\left|\bigcup_{i \in I} A_i\right| \leq \sum_{i \in I} |A_i|.$$

Proof. Map each $a \in \bigcup_{i \in I} A_i$ to $(i, a) \in \bigsqcup_{i \in I} A_i$ for the smallest i such that $a \in A_i$. □

Theorem 4.47. For every infinite well-orderable cardinal κ, we have $\kappa^2 = \kappa$.[29]

Proof. By induction. Suppose for all infinite cardinals $\lambda < \kappa$, we have $\lambda^2 = \lambda$. Then

$$\begin{aligned} \kappa^2 &= |\kappa \times \kappa| \\ &= \left|\bigcup_{\alpha < \kappa} (\alpha \times \alpha)\right| && \text{by Corollary 4.44} \\ &\leq \sum_{\alpha < \kappa} |\alpha|^2 && \text{(cardinal sum, by Proposition 4.46)} \\ &\leq \sum_{\alpha < \kappa} |\alpha|^2 && \text{(ordinal sum, by Remark 4.32)} \\ &\leq \sup_{\alpha < \kappa} \sum_{\beta < \alpha} |\beta|^2 && \text{(ordinal sum and sup, by Corollary 4.44 and Exercise 3.169);} \end{aligned}$$

but for each $\alpha < \kappa$, we have $\left|\sum_{\beta < \alpha} |\beta|^2\right| \leq |\alpha|^3 < \kappa$ by the IH (for $\alpha \geq \omega$) or definition of ω (for $\alpha < \omega$), whence $\sum_{\beta < \alpha} |\beta|^2 < \kappa$ since κ is initial. □

Corollary 4.48. For two well-orderable cardinals κ, λ at least one of which is infinite, we have

$$\begin{aligned} \kappa + \lambda &= \max(\kappa, \lambda), \\ \kappa \cdot \lambda &= \max(\kappa, \lambda) \quad \text{if } \kappa, \lambda \neq 0. \end{aligned}$$

Proof. WLOG λ is infinite and $\kappa \leq \lambda$; then

$$\kappa \sqcup \lambda = \{(i, \alpha) \in 2 \times \lambda \mid i = 0 \implies \alpha \in \kappa\} \subseteq \lambda \times \lambda,$$

whence $\kappa + \lambda \leq \lambda^2 = \lambda$, and clearly also $\lambda \leq \kappa + \lambda$ and $\kappa \cdot \lambda \leq \lambda^2$; if $\kappa > 0$, then also $\lambda = 1 \cdot \lambda \leq \kappa \cdot \lambda$. □

Corollary 4.49. For an infinite well-orderable cardinal κ, we have $\kappa^n = \kappa$ for every $1 \leq n \in \mathbb{N}$. □

[29] More precisely, the proof yields an inductive way of defining an explicit injection $\kappa^2 \hookrightarrow \kappa$ for each κ; hence why this statement for well-orderable κ does not need Choice.

The following is a weird application of well-orderability of $\mathbb{R}$, similar in spirit to the "pathological" constructions using Choice from Section 3.K, but additionally using a bit of cardinal arithmetic:

Theorem 4.50 (Mazurkiewicz)**.** There exists a subset $A \subseteq \mathbb{R}^2$ which contains exactly two points on every line.[30]

Proof. Note that the set $\mathcal{L}$ of lines in $\mathbb{R}^2$ has cardinality $2^{\aleph_0} = |\mathbb{R}|$: for example, we have injections

$$\begin{aligned} \mathbb{R} &\hookrightarrow \mathcal{L} & \mathcal{L} &\hookrightarrow \mathbb{R}^3 \\ b &\longmapsto \{x = b\}, & L &\longmapsto \begin{cases} (1, m, b) & \text{if } L \text{ is a nonvertical line } y = mx + b, \\ (0, 1, b) & \text{if } L \text{ is a vertical line } x = b. \end{cases} \end{aligned}$$

Thus, let $(L_\alpha)_{\alpha < 2^{\aleph_0}}$ be a transfinite enumeration of $\mathcal{L}$, here assuming that $2^{\aleph_0}$ is an initial ordinal. Define a sequence $(A_\alpha \subseteq \mathbb{R}^2)_{\alpha < 2^{\aleph_0}}$, where each $|A_\alpha| \leq 2$, inductively as follows:

- If L_α already contains two points in $\bigcup_{\beta<\alpha} A_\beta$, then $A_\alpha := \varnothing$.
- Otherwise, note that $|\bigcup_{\beta<\alpha} A_\beta| \leq 2 \cdot |\alpha| < 2^{\aleph_0}$, thus also $|(\bigcup_{\beta<\alpha} A_\beta)^2| < 2^{\aleph_0} = |L_\alpha|$. For each pair of distinct points in $\bigcup_{\beta<\alpha} A_\beta$, the unique line through them is not L_α by assumption, hence intersects L_α in at most one point. Pick one or two (depending on whether $|L_\alpha \cap \bigcup_{\beta<\alpha} A_\beta| = 1$ or 0) points on L_α not on any such line and not in $\bigcup_{\beta<\alpha} A_\beta$, and let A_α be those points.

We claim that $A := \bigcup_{\alpha<2^{\aleph_0}} A_\alpha$ works. Indeed, to check that L_α contains exactly two points in A: by definition of A_α, $L_\alpha \cap \bigcup_{\beta\leq\alpha} A_\beta$ contains at least two points. If $L_\alpha \cap A$ contained at least three points, then there is a least β such that $L_\alpha \cap \bigcup_{\gamma\leq\beta} A_\gamma$ contains at least three points, which means $L_\alpha \cap \bigcup_{\gamma<\beta} A_\gamma$ still contains at most two points. But by definition of A_β, we would not have either added a new point to a line that already passes through two existing points, or added two new points to a line (namely $L_\alpha = L_\beta$) that already had a point. □

Another useful consequence of Theorem 4.47 is the following generalization of Proposition 3.180, which recall said that a countable subset of $\mathbb{R}$ generates a countable subgroup, etc.

Corollary 4.51 (assuming Choice)**.** Let $T : \mathcal{P}(X) \to \mathcal{P}(X)$ be a finitary monotone set operator (in the sense of Proposition 3.180), and κ be an infinite cardinal such that T maps finite sets to sets of size $\leq \kappa$. Then for any $A \subseteq X$, we have $|\overline{T}(A)| \leq \max(|A|, \kappa)$.

Proof. Since T is finitary, we have

$$\begin{aligned} |T(A)| &= |\textstyle\bigcup_{n\in\mathbb{N}} \bigcup_{\vec{b}\in A^n} T(\{b_0, \dots, b_{n-1}\})| \\ &\leq \textstyle\sum_{n\in\mathbb{N}} \sum_{\vec{b}\in A^n} |T(\{b_0, \dots, b_{n-1}\})| \\ &\leq \textstyle\sum_{n\in\mathbb{N}} |A|^n \cdot \kappa \\ &\leq \textstyle\sum_{n\in\mathbb{N}} \max(|A|, \kappa) \\ &= \max(|A|, \kappa). \end{aligned}$$

Now by induction, T^n obeys the same bound for each $n \in \mathbb{N}$, thus by Proposition 3.180, so does $\overline{T}(A) = A \cup \bigcup_{n<\omega} T(A_n)$. □

Example 4.52. A $\mathbb{Q}$-vector space X of infinite (well-orderable) dimension κ, or even just with a generating set of cardinality κ, has cardinality κ. Similarly for a κ-generated group, ring, etc.

Example 4.53. An $\mathbb{R}$-vector space of dimension $\kappa \geq 2^{\aleph_0}$ has cardinality κ.

For a further generalization replacing "finitary" with larger arities, see Exercise 4.93.

[30] It appears to be an open problem whether such a set can be constructed without Choice! (It is known that the existence of such a set does not imply that $\mathbb{R}$ is well-orderable; see A. Miller, *Infinite Combinatorics and Definability*.)

4.F. **Regularity, powers, and inaccessibility.** What can we say about the indexed sum and product operations (Definition 4.38)? We henceforth work under full Choice, which is needed even in order for the indexed operations to be well-defined.

Proposition 4.54. Let $(\kappa_i)_{i\in I}$ be a family of cardinals, such that $\sup_{i\in I}\kappa_i \geq \max(|I|,\aleph_0)$. Then

$$\sum_{i\in I}\kappa_i = \sup_{i\in I}\kappa_i.$$

Proof. $\geq$ is straightforward. For $\leq$, we have

$$\begin{aligned}\sum_{i\in I}\kappa_i &\leq \sum_{i\in I}\sup_{j\in I}\kappa_j\\ &= |I|\cdot\sup_{j\in I}\kappa_j\\ &\leq (\sup_{j\in I}\kappa_j)^2\\ &= \sup_{j\in I}\kappa_j.\end{aligned}$$

□

Example 4.55. $\sum_{n\in\mathbb{N}}\aleph_n = \sup_{n\in\mathbb{N}}\aleph_n = \aleph_\omega$.

Example 4.56. Clearly any $\kappa = \sum_{\alpha<\kappa}1$, hence we need the assumption that $\sup_i\kappa_i \geq \max(|I|,\aleph_0)$.

Exercise 4.57. Show that more generally,

$$\sum_{i\in I}\kappa_i = \max(\sup_{i\in I}\kappa_i, |\{i\in I \mid \kappa_i > 0\}|),$$

provided the RHS is infinite. (A version of this was already used in the proof of Theorem 4.47.)

Corollary 4.58. For an infinite cardinal κ and a family of cardinals $(\lambda_i)_{i\in I}$ with $|I|,\lambda_i<\kappa$,

$$\sum_{i\in I}\lambda_i < \kappa \iff \sup_{i\in I}\lambda_i < \kappa.$$

Proof. If the RHS above is finite, then clearly so is the LHS; thus one is $<\kappa$ iff the other is. □

Definition 4.59. A cardinal κ is **regular** if for any family of cardinals $(\lambda_i)_{i\in I}$ with $|I|,\lambda_i<\kappa$, we have $\sum_{i\in I}\lambda_i<\kappa$, or equivalently if κ is infinite, $\sup_{i\in I}\lambda_i<\kappa$.

Exercise 4.60. Show that κ is regular iff for any family of sets $(A_i)_{i\in I}$ with $|I|,|A_i|<\kappa$, we have $|\bigcup_{i\in I}A_i|<\kappa$.

Example 4.61. 0 is (vacuously) regular.

Example 4.62. 1 is regular: any family of cardinals $(\lambda_i)_{i\in I}$ with $|I|<1$ must be empty.

Example 4.63. 2 is regular: any family of cardinals $(\lambda_i)_{i\in I}$ with $|I|,\lambda_i<2$ has sum either 0 or $\lambda_i<2$ for the unique $i\in I$.

Example 4.64. No $3\leq n<\omega$ is regular, since $n=(n-1)+1$.

Remark 4.65. Not everyone agrees on which finite cardinals (if any) are considered regular. (Note that if we instead take $\sup_{i\in I}\lambda_i<\kappa$ as the primary definition, then every $n<\omega$ *except* 0 would be regular.) The definition we have given is the most useful from the perspective of Remark 4.70.

Example 4.66. $\aleph_0$ is regular, being closed under (binary) $+$.

Example 4.67. Any infinite successor cardinal κ^+ is regular: if $|I|,\lambda_i<\kappa^+$, then $|I|,\lambda_i\leq\kappa$, whence $\sum_{i\in I}\lambda_i\leq\kappa^2=\kappa<\kappa^+$.

Example 4.68. $\aleph_\omega=\sum_{n\in\mathbb{N}}\aleph_n$ is *not* regular.

Remark 4.69. The existence of infinite regular cardinals which are not successors, called **weakly inaccessible cardinals**, other than $\aleph_0$, is not provable in ZFC. The reason is related to (but slightly subtler than) Exercise 4.90: for such κ, a "definable subuniverse" of V_κ called L_κ, in which GCH (Theorem 4.72) holds (thus "weakly inaccessible" becomes "strongly inaccessible"), would be a model of ZFC. See also Theorem 4.72.

Remark 4.70. In ordinary mathematics, regular cardinals are precisely the meaningful "arity bounds" on types of operations we can equip a set with. For example:

- A group, ring, vector space, etc., has only *finitary* operations, meaning arities $< \aleph_0$.
- For a fixed group G, a G-set (set equipped with group action) has only *unary* operations, meaning arities < 2. More things are true about such structures: for example, the substructures (subsets closed under the operations) are closed under unions, as well as intersections.
- The Borel sets in $\mathbb{R}$ (Example 3.184) are closed under countable Boolean operations, which have arities $< \aleph_1$.
- It does not really make sense to consider only operations of arities < 3, say, because we can compose a binary operation $*$ to get a quaternary operation $(a * b) * (c * d)$.
- Similarly, it does not make sense to consider operations of arities $< \aleph_\omega$, because we can compose a countable operation with ones of arities $\aleph_0, \aleph_1, \aleph_2, \dots$ to get an $\aleph_\omega$-ary operation.
- For any regular cardinal κ, there are good notions of **κ-Borel set** (ones built from intervals via Boolean operations of size $< \kappa$), **κ-ary first-order logic** $\mathcal{L}_{\kappa\omega}$ (with conjunctions $\bigwedge$ and disjunctions $\bigvee$ of size $< \kappa$), etc.

In general, we say that a monotone set operator $T : \mathcal{P}(X) \to \mathcal{P}(X)$ is $< \kappa$**-ary**[31] if whenever $x \in T(A)$, then $x \in T(B)$ for some $B \subseteq A$ with $|B| < \kappa$.

Exercise 4.71. Let $\kappa \geq 2$ be a cardinal.

(a) Show that if κ is regular, then $< \kappa$-ary monotone set operators are closed under composition.
(b) Show that the converse holds as well. [Hint: close under $< \kappa$-ary unions in a powerset.]
(c) Show that $< \kappa$-ary monotone set operators are always closed under arbitrary pointwise unions: if $T_i : \mathcal{P}(X) \to \mathcal{P}(X)$ is $< \kappa$-ary, then so is $(\bigcup_i T_i)(A) := \bigcup_i T_i(A)$.
(d) Conclude that if κ is regular and T is $< \kappa$-ary, then so is $\overline{T}$ (cf. Proposition 3.180). Moreover, the transfinite sequence $A = A_0 \subseteq A_1 \subseteq \cdots$ from Theorem 3.176 stabilizes at $A_\kappa = \overline{T}(A)$.

Regularity also plays an important role in cardinal exponentiation and more generally, indexed products. Recall that by Cantor's Theorem 4.35, $\kappa < 2^\kappa$ for every κ; thus $2^\kappa \geq \kappa^+$.

Continuum Hypothesis (CH). $|\mathbb{R}| = 2^{\aleph_0} = \aleph_1$.

Generalized Continuum Hypothesis (GCH). For every infinite cardinal κ, $2^\kappa = \kappa^+$.

Theorem 4.72 (Gödel)**.** If ZFC is consistent, then so is ZFC + GCH, i.e., GCH cannot be disproved.

Proof idea. Take the ZFC universe V. Roughly speaking, GCH might fail because for a set X, Comprehension says it must have certain subsets; but it may have many more than just those. Gödel constructed a subuniverse $L \subseteq V$, the **constructible universe**, via an inductive procedure analogous to the cumulative hierarchy (Section 3.J) but adding at each level only those subsets of the previous level demanded by Comprehension, i.e., which are definable by a formula $\phi(x)$. Since there are only countably many formulas, each $X \in L$ will have the least possible $2^{|X|} = |X|^+$. □

Theorem 4.73 (Easton)**.** Assume ZFC is consistent. Let F be any (proper class) function from infinite regular cardinals to infinite regular cardinals such that

(i) $\kappa \leq \lambda \implies F(\kappa) \leq F(\lambda)$;
(ii) $\kappa < F(\kappa)$.

Then it is consistent with ZFC that $2^\kappa = F(\kappa)$ for all infinite regular κ.

[31] This usually gets abbreviated to "κ-ary", leading to potential confusion since $\kappa \not< \kappa$. For example, "2-ary", i.e., < 2-ary, means nullary or unary, but *not* binary.

Example 4.74 (Cohen)**.** In particular, CH cannot be proved from ZFC: we could declare $2^{\aleph_0} := \aleph_2$, say, and inductively for each regular $\kappa > \aleph_0$, $2^\kappa :=$ the least regular $> 2^\lambda$ for all $\lambda < \kappa$.

Remark 4.75. The assumption of regularity in Easton's Theorem 4.73 may seem to come from nowhere, but it is needed. A theorem of Silver says that GCH cannot first fail at $\aleph_{\omega_1} = \sup_{\alpha<\omega_1} \aleph_\alpha$! The possible behaviors of cardinal exponentiation at *singular* (i.e., non-regular) cardinals is quite subtle, and is a focus of modern set theory research (see e.g., Shelah's *pcf theory*).

Easton's theorem tells us that in ZFC, expressions of the form 2^κ essentially cannot be "evaluated" into any simpler form; they behave like "indeterminates", whose values may vary from universe to universe. But given these "indeterminates", we can evaluate many other powers and products.

Proposition 4.76. If λ is an infinite cardinal and $\mu \leq \kappa \leq \mu^\lambda$, then $\kappa^\lambda = \mu^\lambda$.

Proof. $\mu^\lambda \leq \kappa^\lambda \leq (\mu^\lambda)^\lambda = \mu^{\lambda^2} = \mu^\lambda$. □

This allows us to "evaluate" κ^λ as long as κ is not too big relative to λ. Namely, if $2 \leq \kappa \leq 2^\lambda$, then $\kappa^\lambda = 2^\lambda$. More generally, we may inductively "evaluate" κ^λ in terms of μ^λ for $\mu < \kappa$, *unless* the cardinals $< \kappa$ are closed under $(-)^\lambda$; in particular, $\kappa > 2^\lambda > \lambda$. In that case, we may attempt to use instead:

Proposition 4.77. If κ is regular, λ is infinite, $\kappa > \lambda$, and $\mu^\lambda \leq \kappa$ for all $\mu < \kappa$, then $\kappa^\lambda = \kappa$.

Proof. Since $\kappa > \lambda$ is regular, every function $f : \lambda \to \kappa$ must land in $\sup^+_{\alpha\in\lambda} f(\alpha) < \kappa$. Thus

$$\begin{aligned} \text{(cardinal power) } \kappa^\lambda &= \left|\bigcup_{\alpha<\kappa} \alpha^\lambda\right| \quad \text{(set of functions)} \\ &\leq \sum_{\alpha<\kappa} |\alpha|^\lambda \quad \text{(cardinal power)} \\ &\leq \kappa^2 = \kappa. \end{aligned}$$

□

Exercise 4.78. If κ above is singular, but the cardinals $< \kappa$ are still closed under sums of size $\leq \lambda$ (cf. **??**), then the above still holds.

Example 4.79. For any $2 \leq \kappa \leq 2^{\aleph_0}$, we have $\kappa^{\aleph_0} = 2^{\aleph_0}$ (generalizing Example 4.37). For example, there are just as many functions $\mathbb{R} \to \mathbb{R}$ as there are subsets of $\mathbb{R}$.

In particular, $\aleph_1^{\aleph_0} = 2^{\aleph_0}$.

If CH holds, then this is $= \aleph_1 < \aleph_2$, whence the cardinals $< \aleph_2$ are closed under $(-)^{\aleph_0}$, whence $\aleph_2^{\aleph_0} = \aleph_2$, whence similarly $\aleph_3^{\aleph_0} = \aleph_3$, etc., up to $\aleph_\omega^{\aleph_0}$ which we can't compute since $\aleph_\omega$ isn't regular. (It turns out that $\aleph_\omega^{\aleph_0} > \aleph_\omega$ always, while $\aleph_\omega^{\aleph_0}$ can be quite large; see **??**.)

If CH fails, then $2^{\aleph_0} \geq \aleph_2$, whence $\aleph_2^{\aleph_0} = 2^{\aleph_0}$. Similarly to the case of CH, if now $2^{\aleph_0} = \aleph_2$, then $\aleph_3^{\aleph_0} = \aleph_3$, $\aleph_4^{\aleph_0} = \aleph_4$, etc.

Exercise 4.80 (Hausdorff formula)**.** For $\kappa \geq 2$ and $\lambda \geq \aleph_0$, we have $(\kappa^+)^\lambda = \max(\kappa^\lambda, \kappa^+)$.

Concerning indexed products $\prod_{i\in I} \kappa_i$, we may reduce them to powers:

Example 4.81. $\overbrace{2 \cdot 2 \cdot \cdots}^{\aleph_0} \cdot \aleph_\omega \cdot \aleph_\omega = 2^{\aleph_0} \cdot \aleph_\omega$ is a product of $\aleph_0$ many cardinals $\leq \aleph_\omega$, which may however be strictly less than $\aleph_\omega^{\aleph_0}$, e.g., if CH holds (see Example 4.79).

In this example, we have a product $\prod_{i\in I} \kappa_i$ where most of the κ_i's are bounded below $\sup_i \kappa_i$; we may then reduce inductively to computing a product of smaller cardinals $\prod_{j\in J} \kappa_j$ where $\sup^+_{j\in J} \kappa_j < \sup^+_{i\in I} \kappa_i$, as well as a smaller product $\prod_{i\in I\setminus J} \kappa_i$ where $J \subseteq I$ with $|I \setminus J| < |I|$, and then multiplying these two together. (That is, we are inducting lexicographically on $(|I|, \sup^+_{i\in I} \kappa_i)$.) In the remaining case, most of the κ_i's are big; then we may apply the following.

Proposition 4.82. Let $(\kappa_i)_{i\in I}$ be a family of nonzero cardinals, such that for each i, we have $|\{j \in I \mid \kappa_j \geq \kappa_i\}| = |I|$. Then

$$\prod_{i\in I} \kappa_i = (\sup_{i\in I} \kappa_i)^{|I|}.$$

Proof. $\leq$ is straightforward; we show $\geq$. WLOG $I = |I|$ is an initial ordinal. If I is finite, both sides are 1 (if $I = 0$) or $\max_i \kappa_i$; so assume I is infinite. Let $p : I \times I \cong I$ be a bijection. Define $q : I \times I \hookrightarrow I$ by induction on $p(i, j)$ as follows: $q(i, j) \in I$ is least so that

$$\kappa_{q(i,j)} \geq \kappa_j, \qquad q(i, j) \neq q(i', j') \quad \forall p(i', j') < p(i, j);$$

this is possible because by assumption, there are I-many κ's which are $\geq \kappa_j$, while there are only $|p(i, j)| < I$-many (i', j')'s with $p(i', j') < p(i, j)$. Then because each $\kappa \neq 0$,

$$\begin{aligned}\prod_{i\in I} \kappa_i &\geq \prod_{i\in \mathrm{im}(q)} \kappa_i \\ &= \prod_{(i,j)\in I\times I} \kappa_{q(i,j)} \\ &\geq \prod_{i\in I} \prod_{j\in I} \kappa_j \\ &\geq \prod_{i\in I} \sup_{j\in I} \kappa_j\end{aligned}$$

(using various laws for indexed products from Exercises 4.41 and 4.42). □

Exercise 4.83. Verify that indeed, for each product of nonzero cardinals $\prod_{i\in I} \kappa_i$, either the above result applies, or we may reduce to two products $\prod_{j\in J} \kappa_j$ where either $|J| < |I|$, or $|J| = |I|$ and $\sup^+_{j\in J} \kappa_j < \sup^+_{i\in I} \kappa_i$ (again using associative/commutative laws).

Definition 4.84. A cardinal κ is a **strong limit** if it is infinite[32] and:

- for any $\lambda < \kappa$, we have $\lambda^\lambda < \kappa$;
- equivalently, for any $\lambda, \mu < \kappa$, we have $\lambda^\mu < \kappa$;
- equivalently, for any sets A, B of size $< \kappa$, we have $|A^B| < \kappa$;
- equivalently, for any $\lambda < \kappa$, we have $2^\lambda < \kappa$;
- equivalently, for any set A of size $< \kappa$, we have $|\mathcal{P}(A)| < \kappa$.

By Cantor's theorem, these imply that κ is a **weak limit**, i.e., $0 < \kappa$ and $\lambda < \kappa \implies \lambda^+ < \kappa$.

Example 4.85. $\aleph_0$ is a strong limit.

Example 4.86. The next strong limit is $\sup\{\aleph_0, 2^{\aleph_0}, 2^{2^{\aleph_0}}, 2^{2^{2^{\aleph_0}}}, \dots\}$.

Remark 4.87. The **beth cardinals** are $\beth_0 := \omega$, $\beth_1 := 2^\omega$, $\beth_2 := 2^{2^\omega}$, …, $\beth_\alpha := \sup_{\beta<\alpha} 2^{\beth_\beta}$.

Thus, for any limit ordinal α, $\beth_\alpha$ is a strong limit cardinal (and $\aleph_\alpha$ is a weak limit cardinal).

The GCH can be stated as: $\aleph_\alpha = \beth_\alpha$.

While regularity means that sets of size $< \kappa$ are closed under $\bigcup$, strong limit means they are closed under $\mathcal{P}$; these are the two fundamental set-theoretic operations. Combining them yields

Definition 4.88. A cardinal κ is **strongly inaccessible** if it is regular and a strong limit.

Exercise 4.89. Show that κ is strongly inaccessible iff it is infinite and for any family of cardinals $(\lambda_i)_{i\in I}$ with $|I|, \kappa_i < \kappa$, we have $\prod_{i\in I} \lambda_i < \kappa$.

As the name suggests, strongly inaccessible cardinals are called such because they are so large that other than $\aleph_0$, none of them can be constructed in ZFC. This is because the "things below them" are closed under everything that ZFC requires; thus if we had a strongly inaccessible κ, we may simply truncate the universe at κ to get a smaller universe without any strongly inaccessibles. (Similarly, $\aleph_0$ could not be constructed either; we had to declare its existence via the Axiom of Infinity, without which V_ω could as well be the entire universe.)

[32] I suppose that in some contexts, it may also be useful to regard 2 as a strong limit.

Exercise 4.90. A set A is **hereditarily of size** $< \kappa$ if it, its elements, its elements' elements, etc., are all of size $< \kappa$. In other words, every set in the transitive closure $\bigcup\{A\}$ (Definition 3.189) is of size $< \kappa$. Let H_κ be the class of all sets hereditarily of size $< \kappa$.

(a) Prove that $H_\kappa \subseteq V_\kappa$ for every infinite regular cardinal κ. In particular, H_κ is a set.
(b) Prove that $V_\kappa \subseteq H_\kappa$ for every strong limit cardinal κ. Thus, $H_\kappa = V_\kappa$ if κ is strongly inaccessible.
(c) Prove the converses of (a) and (b) (assuming κ is an infinite cardinal).
(d) Verify that $H_\kappa = V_\kappa$ for strongly inaccessible κ has the following properties:
  (i) H_κ is transitive.
  (ii) $\varnothing \in H_\kappa$, and $a, b \in H_\kappa \implies \{a, b\} \in H_\kappa$.
  (iii) If $I \in H_\kappa$ and $(A_i)_{i\in I} \in H_\kappa^I$, then $\bigcup_{i\in I} A_i \in H_\kappa$.
  (iv) $A \in H_\kappa \implies \mathcal{P}(A) \in H_\kappa$.
  (v) $A \subseteq B \in H_\kappa \implies A \in H_\kappa$.
  (vi) For any $A \in H_\kappa$ and function $f : A \to H_\kappa$, we have $f[A] \in H_\kappa$.
  (vii) $A \in H_\kappa \implies \bigcup A \in H_\kappa$.
  (viii) $A, B \in H_\kappa \implies A \times B, B^A \in H_\kappa$.
  (ix) If $I \in H_\kappa$ and $(A_i)_{i\in I} \in H_\kappa^I$, then $\prod_{i\in I} A_i, \bigsqcup_{i\in I} A_i \in H_\kappa$.
  (x) If κ is uncountable, then $\mathbb{N} \in H_\kappa$.
(e) Conclude that H_κ satisfies $\mathsf{ZFC} - \mathsf{Infinity}$ (assuming the real universe does), and ZFC if κ is uncountable.
(f) Note that for $A \in H_\kappa$, not only do we have $\mathcal{P}(A) \in H_\kappa$, but also that H_κ thinks that $\mathcal{P}(A)$ is the powerset of A. Explain why this might not be the case if, say, we did not have (i).
(g) Verify that for any $A \in H_\kappa$, H_κ thinks that A is an ordinal iff A is indeed an ordinal.
(h) Verify that for any $A \in H_\kappa$, H_κ thinks that A is an initial ordinal iff A is indeed such.
(i) Verify that for any $A \in H_\kappa$, H_κ thinks that A is a strongly inaccessible cardinal iff A is indeed such.
(j) Conclude that $\mathsf{Infinity}$ cannot be proved from $\mathsf{ZFC} - \mathsf{Infinity}$, and that the existence of a strongly inaccessible cardinal cannot be proved from ZFC.
(k) Prove that sets U with the above properties (i)–(iv) (called **Grothendieck universes**) are precisely all H_κ for strongly inaccessible κ.

Grothendieck universes are used in areas of math that need to work with "mathematical universes" as mathematical objects, e.g., category theory (the category of all groups, etc.).

In "ordinary" math, one rarely needs such "universes" that are closed under products of the same arity as themselves. Rather, one sometimes wants a collection of "sufficiently small sets" that is closed under products of some *fixed* arities, e.g., under all countable products. For finite products, sets of size $<$ any infinite κ will do (by Theorem 4.47). For infinite products, we may use

Proposition 4.91. For any cardinal λ, there are arbitrarily large regular κ such that for all $|I| \leq \lambda$ and $(\mu_i)_{i\in I}$ where each $\mu_i < \kappa$, we have $\prod_{i\in I} \mu_i < \kappa$.

Proof. We may assume λ is infinite; then any κ of the form $(\kappa_0^\lambda)^+$ will do. □

Example 4.92. For $\lambda = \aleph_0$, this says that there are arbitrarily large regular κ such that a countable product of cardinals $< \kappa$ is still $< \kappa$. For such κ, we have that if $\mathcal{A} \subseteq \mathcal{P}(X)$ is a collection of subsets of size $< \kappa$, then the closure of $\mathcal{A}$ under countable Boolean operations still has size $< \kappa$. For example, $\kappa = (2^{\aleph_0})^+$ works, yielding that there are $2^{\aleph_0}$ Borel subsets of $\mathbb{R}$ (see Example 3.184).

Exercise 4.93. Let $\kappa \geq \lambda$ be infinite regular cardinals such that the conclusion of Proposition 4.91 holds, and let $T : \mathcal{P}(X) \to \mathcal{P}(X)$ be a $< \lambda$-ary monotone set operator (see Exercise 4.71) which maps sets of size $< \lambda$ to sets of size $< \kappa$. Show that $\overline{T}$ maps sets of size $< \kappa$ to sets of size $< \kappa$ (cf. Proposition 3.180).

4.G. **A taste of descriptive set theory.** The independence of the Continuum Hypothesis means that the most familiar uncountable cardinality outside of logic, namely $2^{\aleph_0}$, may or may not be the same as the smallest uncountable cardinality ω_1. Now, unless you've studied logic before, there's a good chance you've never even heard of ω_1; and indeed, every concrete example of a set you've seen is probably provably either countable or has cardinality $\geq 2^{\aleph_0}$. Why is this so?

Exercise 4.94. Try to think of a subset of $\mathbb{R}$ which is uncountable but does not appear to easily admit an injection from $\mathcal{P}(\mathbb{N})$.

You will likely fail, because this cannot be the case for any subset of $\mathbb{R}$ you can easily write down:

Exercise 4.95. Explicitly write down an injection from $\mathcal{P}(\mathbb{N})$ into the set of normal numbers $x \in \mathbb{R}$ (see Example 3.184).

Exercise 4.96. Explicitly define an injection from $\mathcal{P}(\mathbb{N})$ into the set of real numbers whose digits (in base 10, or base 36) contain the complete works of Shakespeare (encoded e.g., in ASCII).

The simplest sets of reals are intervals. An **open** set of reals is a union of open intervals (a, b).

Remark 4.97. For any $a < b$, we have a bijection $(a, b) \cong \mathbb{R}$, given by some shifted/scaled version of arctan. Thus, any open set is either countable (indeed empty) or admits an injection from $\mathbb{R}$ (which in turn admits an injection from $\mathcal{P}(\mathbb{N})$, by Example 4.36).

The next simplest are the **closed** sets: the complements of open sets. The name reflects the fact that these are precisely the sets closed under limits (of sequences).

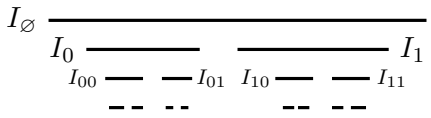
Theorem 4.98 (perfect set theorem)**.** For any uncountable closed set $A \subseteq \mathbb{R}$, we can explicitly define an injection $f : 2^{\mathbb{N}} \hookrightarrow A$. Moreover, the injection is monotone with respect to the lexicographical order on $2^{\mathbb{N}}$, and continuous: $\forall \varepsilon > 0\, \exists n \in \mathbb{N}\, \forall x, y \in 2^{\mathbb{N}}\, (x|n = y|n \implies |f(x) - f(y)| \leq \varepsilon)$.

Proof. First, the intersection of A with some finite closed interval $I = [a, b]$ must be uncountable. Indeed, otherwise $A \cap [n, n+1]$ would be countable for each $n \in \mathbb{Z}$, and so A would be the countable union of these. Moreover, by replacing $n + 1$ with $n + 1/m$ for some $m > 0$, we may require I to have arbitrarily small (positive) length.

Next, whenever $A \cap [a, b]$ is uncountable for some $a < b$, then there must exist $c \in [a, b]$ such that $A \cap [a, c], A \cap [c, b]$ are both uncountable. Indeed, let $a' := \sup\{x \in [a, b] \mid |A \cap [a, x]| \leq \aleph_0\}$; then there is a countable sequence $x_0 < x_1 < \cdots$ converging to a', whence $A \cap [a, a') \subseteq \bigcup_{n \in \mathbb{N}} (A \cap [a, x_n])$ is countable, whence $A \cap [a', b]$ is uncountable. Similarly, letting $b' := \inf\{x \in [a', b] \mid |A \cap [x, b]| \leq \aleph_0\}$, $A \cap [a', b']$ is uncountable. Then any $c \in [a', b']$ works.

Applying this argument again to $[c, b]$, we get that whenever $A \cap [a, b]$ is uncountable, there are disjoint closed subintervals $I, J \subseteq [a, b]$, I to the left of J, namely $[a, c]$ and $[d, b]$ for some $a < c < d < b$, such that both $A \cap I$ and $A \cap J$ are uncountable. Moreover, we may then further shrink I, J to make them as short as we want.

Now let $I_\varnothing = [a_\varnothing, b_\varnothing]$ be the initial interval with $A \cap I_\varnothing$ uncountable, WLOG with $b_\varnothing - a_\varnothing \leq 1$. Define subintervals $(I_s)_{s \in \bigcup_{n \in \mathbb{N}} 2^n}$ by induction on n: given $I_s = [a_s, b_s]$ for $s \in 2^n$ with $A \cap I_s$ uncountable, find $I_{s0}, I_{s1} \subseteq I_s$ of length $\leq 2^{-(n+1)}$ and $A \cap I_{s0}, A \cap I_{s1}$ uncountable, with $I_{s0} < I_{s1}$.



Then for each $x \in 2^{\mathbb{N}}$, $f(x) := \sup_{n \in \mathbb{N}} a_{s|n}$ is the unique point in $\bigcap_{n \in \mathbb{N}} I_{s|n}$, and is in A because it is distance $\leq 2^{-n}$ (= length of $I_{s|n}$) away from a point in $A \cap I_{s|n}$ for each n and A is closed. Moreover, f is monotone since for $x <_{\text{lex}} y$, we have $f(x) \in I_{x|(n+1)} < I_{y|(n+1)} \ni f(y)$ for the least n such that $x(n) \neq y(n)$; and f is continuous since $x|n = y|n \implies |f(x) - f(y)| \leq 2^{-n}$. □

Example 4.99. Consider $A := \{x \in \mathbb{R} \mid \sin(\cos(x^2 - \pi^x)) \leq x^3 - x + 1\}$. I have no idea what this set is, or even if it's nonempty; but I do know that it cannot be a counterexample to the CH. Moreover, if it's uncountable, then there is a continuous injection $f : 2^{\mathbb{N}} \to A$, which is "explicitly definable" since it suffices to specify $f(x)$ at the countably many $x \in 2^{\mathbb{N}}$ with only finitely many 1's.

In fact, the scope of the perfect set theorem is much broader:

Exercise 4.100. A G_δ **set** is a countable intersection of open sets $\bigcap_{n\in\mathbb{N}} U_n$. By replacing each U_n with $\bigcap_{m\leq n} U_m$, we may assume $U_0 \supseteq U_1 \supseteq \cdots$.

(a) Verify that each closed set $A \subseteq \mathbb{R}$ is G_δ. [Consider the nearest distance to A.]
(b) Prove the perfect set theorem for G_δ sets. [Modify the above argument to ensure that each I_s for $s \in 2^n$ is contained in one of the open intervals making up U_n.]
(c) Verify that $A := \{x \in \mathbb{R} \mid$ every finite string of digits appears once in the digits of $x\}$ is G_δ. Can you think of an explicit injection $2^{\mathbb{N}} \hookrightarrow A$?

Call $A \subseteq \mathbb{R}$ **soluble** if there is a G_δ set $X \subseteq \mathbb{R}$ and a continuous bijection $g : X \to \mathbb{R}$ such that $g^{-1}[A] \subseteq X$ is closed (under limits that exist in X).

(d) Prove that if $A \subseteq \mathbb{R}$ is soluble, then the perfect theorem holds for A: either A is countable, or there is a continuous injection $f : 2^{\mathbb{N}} \to A$ (we cannot require monotonicity in general).
(e) Verify that closed sets are soluble.
(f) Prove that open sets are soluble. [Consider $\exp[A] \cup -\exp[\mathbb{R} \setminus A]$.]
(g) Prove that a complement of a soluble set is soluble. [Apply (f) to $\mathbb{R} \setminus \overline{g^{-1}[A]}$.]
(h) Suppose $A \subseteq \mathbb{R}$ such that for every G_δ set $X \subseteq \mathbb{R}$ and continuous bijection $g : X \to \mathbb{R}$, $g^{-1}[A]$ is soluble, and moreover $B \subseteq \mathbb{R}$ also has this property. Prove that $A \cup B$ then also has this property.
(i) Moreover, if $A_0 \subseteq A_1 \subseteq \cdots \subseteq \mathbb{R}$ all have this property, then so does $\bigcup_{n\in\mathbb{N}} A_n$.
(j) All Borel sets (Example 3.184) are soluble, hence the perfect set theorem holds for them.
(k) (hard) All soluble sets are Borel.

Descriptive set theory in general studies the properties of these kinds of "explicitly definable" sets. The perfect set property, a strong form of CH, is one among a long list of nice properties one can prove for such sets but not for arbitrary sets: for example, many of the pathological constructions using Choice from Section 3.K also disappear.